1

Richard J. Levernier
P.O. Box 146
Germantown, MD 20875

December 7, 2005

Honorable Scott Bloch
Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW
Washington, DC 20036

Dear Mr. Bloch,

This letter is in response to an email from your office indicating that your review of my whistleblower disclosure (OSC File No. DI-02-0572), the subsequent DOE report, and my additional comments is imminent.

After the Special Counsel determined there was a "substantial likelihood" that the information contained in my disclosure constituted a substantial and specific danger to public health and safety, the Secretary of Energy submitted the required report of investigation to OSC in May 2003. DOE concluded that my disclosures were unfounded, dated, and that they did not constitute a danger to public health and safety.

However, in the two and a half years since DOE issued this conclusion, no less than a dozen relevant, internal and external security reviews of DOE corroborated many of the issues I raised in my January 2002 whistleblower disclosure. In my opinion, any objective and reasonable person evaluating my whistleblower disclosures, the DOE dismissal of my disclosures, and the subsequent, directly relevant reports would find the DOE report seriously lacking in credibility.

I believe the DOE report should be returned to DOE with recommendations that the agency take the necessary corrective actions to resolve long-standing and well-documented security deficiencies. This is an opportunity for the Special Counsel to have a substantial positive impact on the national security of this country.

However, if, despite the overwhelming documented evidence, you decide to accept the DOE Report as reasonable, **I would like all of my comments (and the additional attachments included in my correspondence with your office) included in the public file on my disclosure**. I understand that, according to the relevant statute (5 USC Sec. 1219), you are not specifically required to include my comments in the public file. But, this very limited interpretation of the statute badly misses Congress's intent to make available a file in which the public can inform themselves completely on issues of public health and safety. Including only agency rebuttals in these files compromises your Office's mission and integrity.

Moreover, your office informed me, in writing, on October 25, that "The [DOE] report and your comments will be transmitted to the President and appropriate congressional oversight committees, *and will be maintained by OSC in a public file.*" You have my absolute consent to include my comments in the public file, as you have stated you would.

Sincerely,

Richard J. Levernier

Richard J. Levernier

2

Richard J. Levernier
PO Box 146
Germantown, MD 20875

December 19, 2003

Catherine A. McMullen, Esq.
Chief, Whistleblower Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, NW
Washington, DC 20036

Via Certified Mail #7099 3400 0005 4288 5691

Dear Ms. McMullen:

The purpose of this letter is to provide my comments on the U.S. Department of Energy (DOE) report concerning my whistleblower disclosure. On January 15, 2002, I submitted a whistleblower disclosure to the U.S. Office of Special Counsel (OSC) (File No. DI-02-0572). On October 25, 2002, the OSC determined that there was a "substantial likelihood" that the information contained in my disclosure constituted a substantial and specific danger to public health and safety arising out of actions taken or not taken by officials at DOE concerning physical security at DOE's nuclear weapons facilities. Therefore, OSC transmitted the allegations to the Secretary of Energy for an investigation and report pursuant to 5 USC 1213 (c). Pursuant to the statute, the Secretary has 60 days to conduct an investigation of these allegations and report back to OSC. DOE requested and OSC granted numerous extensions of the established 60 day deadline. Finally, on May 29, 2003, (more than 5 months beyond the initial deadline) the Secretary of Energy submitted the required report of investigation to OSC.

On December 2, 2003, I was contacted by OSC, through my legal counsel, and informed that the DOE report (25 pages in length) was available for my review and comment. Please explain the delay and the OSC's authority to withhold the report from me for over six months. My attorney has been unable to obtain a response to this query. OSC informed me that the DOE report was marked "Sensitive Information – For Official Use Only" and that a copy could not be provided to me and I would only be allowed to review the document in the OSC offices with an OSC observer present. I was also informed that my attorney could not have access to the DOE report. This was a surprising development since my disclosure was unclassified and OSC had informed me, in writing, on October 25, 2002, that "The report and your comments will be transmitted to the President and appropriate congressional oversight committees, and will be maintained by OSC in a public file." Please explain the legal basis under the Whistleblower Protection Act to withhold an unclassified report transmitted under 5 USC 1213 from the public record. I requested the opportunity to review the OSC referral of my whistleblower disclosure to DOE in order understand how my issues were framed by OSC for DOE investigation. My request to review the OSC referral was denied. Please explain the legal authority and

public policy basis under the Whistleblower Protection Act and 5 USC 1213 for the OSC to keep secret from me the way OSC translated my charges and which it deemed worthy of investigation.

My whistleblower disclosure to OSC was 36 pages in length with 22 supporting attachments. During the DOE investigation I was contacted and asked to provide additional information. In response to the DOE request of January 6, 2003, I submitted a 39 page statement with 14 supporting attachments on January 13, 2003.

My whistleblower disclosure included the following security deficiencies at DOE nuclear weapons facilities:

- Lack of explosive detection capability at all critical facility entry points
- Unrealistic and simplistic protective force performance tests
- Capabilities of adversaries not accurately represented in performance tests
- Protective force performance test scenarios are not worst case
- The "shock value" of a terrorist attack is undervalued by DOE
- DOE primarily tests using theft scenarios; these are easier than sabotage to defend
- Performance test evaluators are not always qualified to evaluate tactics and effectiveness
- Performance test laser equipment (MILES) is obsolete and/or not maintained
- Comprehensive records of performance tests are not maintained
- DOE "adversary teams" are unqualified as "terrorists" for testing purposes; military special operations personnel are only used infrequently
- Cheating on performance tests is common and not thoroughly investigated
- Computer modeling of protective force tactics, while recognized as valuable, is underutilized and not required
- Comprehensive oversight of safeguards and security is ineffective
- Field offices inspect and rate themselves during the required annual security surveys
- Security survey inspectors are frequently unqualified and only "inspect" part-time
- Vulnerability assessments are flawed due to a number of factors and are not standardized
- Unannounced inspections are not a component of security oversight
- Some security management personnel are unqualified
- Security deficiencies are not properly managed until resolved
- Required corrective action plans and root cause analyses are not always developed, approved and tracked
- Critical risk issues at facilities are not always resolved
- The DOE Design Basis Threat (DBT) severely underestimates the threat posed by terrorists

The cumulative impact of these acute inter-related deficiencies is that the national security assets entrusted to DOE are not adequately protected.

The DOE report states that the allegations contained in my whistleblower disclosure (summarized above) are completely unfounded and that there is no substantial and specific danger to public health and safety. The DOE report states that my disclosure contains outdated information and that numerous improvements have been made since my disclosure.

In order to meet the minimum statutory requirements of 5 USC 1213(e)(2)(b), section 1213(d) requires the following:

> "Any report required under subsection (c) shall be reviewed and signed by the head of the agency and shall include –
>
> (1) a summary of the information with respect to which the investigation was initiated;
> (2) a description of the conduct of the investigation;
> (3) a summary of any evidence obtained from the investigation;
> (4) a listing of any violation or apparent violation of any law, rule, or regulation; and
> (5) a description of any action taken or planned as a result of the investigation, such as -
> (A) changes in agency rules, regulations, or practices;
> (B) the restoration of any aggrieved employee;
> (C) disciplinary action against any employee; and
> (D) referral to the Attorney General of any evidence of a criminal violation.

The report does not meet minimum legal standards for completeness required by subsections 2 and 3 above. Indeed, there was not even an attempt to comply with these provisions. The report is silent on the methodology and evidentiary basis for its conclusions.

The essence of the report's approach is to describe DOE policies as the baseline for an effective security system, and then conclude that since my allegations describe contrary practices, I must be wrong. That begs the question. The point of my disclosure is that the paper policies are being systematically violated in the field. The agency takes at face value reassurances from its Office of Independent Oversight. But there is no basis to accept those conclusions beyond blind faith. How did the Office come to those conclusions? Indeed, one of my primary charges was that this same Office has been ineffective and unreliable. DOE's approach is the equivalent of mimicking a defendant's unsupported innocent plea without requiring an explanation.

Nor did DOE offer any evidence to support the innocent verdict it gave itself. This is understandable, since the agency declined to act on my offer to provide supporting witnesses for all my charges. In short, the report's failure to disclose its methodology or evidentiary basis renders its conclusions not only incomplete, but arbitrary and meaningless.

Further, there is evidence that DOE's asserted conclusions are unreasonable. DOE's assertion that my allegations are unfounded and that there is no substantial and specific danger to public health and safety is unreasonable, because it is false.[1] The U.S General Accounting Office (GAO) issued GAO-03-896TNI (copy attached) Testimony Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform, "DOE Faces Security Challenges in the Post September 11, 2001 Environment" on June 24, 2003. The GAO testimony is an unclassified, open source document, available to the public on the internet and contains current information developed by a credible and independent organization with widely recognized nuclear security expertise. **Contrary** to the DOE report the GAO says, "Over the past decade, we and others have raised concerns about the adequacy of security at nuclear weapons facilities within the department and National Nuclear Security Administration (NNSA). For example, we reported to you last month that NNSA needs to better manage its safeguards and security program." (GAO-03-471; *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, May 30, 2003)

The GAO testimony states,

"In summary, we found NNSA has not been fully effective in managing its safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from adversaries seeking to inflict damage. Specifically we found the following:

- NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations.

- Without a stable and effective management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA site offices on how they assess contractors' security activities. NNSA cannot be assured that that all facilities are subject to the comprehensive annual assessments that DOE policy requires.

- To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or the cost versus benefit of taking corrective action.

- NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for site offices to effectively oversee security activities.

---

[1] To illustrate the games being played, when the probe began the initial senior executive security manager assigned to conduct the investigation, John Todd, reassured me and openly acknowledged that my concerns were long-standing, well-known problems. Somehow, that assessment was transformed into, "Nothing's wrong", after Mr. Todd's retirement in the middle of the investigation.

With respect to DOE's and NNSA's responses to the September 11 terrorist attacks we found that the department has taken a number of important steps to respond to the terrorist threat; however, DOE's response has been slow in some vital respects, and DOE and NNSA will need at least several years and an as yet undetermined amount of resources before their sites are fully prepared to meet the projected threat. Specifically, we found the following:

- DOE and NNSA took immediate steps to improve security in the aftermath of the September 11 terrorist attacks. For example, DOE and NNSA moved to a higher level of security that required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.

- The number and capabilities of the terrorists involved in the September 11 attacks rendered obsolete DOE's DBT, last issued in 1999. However, DOE's effort to develop and issue a new DBT took almost 2 years; it issued the new DBT in May 2003. The effort to develop a new DBT was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.

- Successfully addressing the increased threats contained in the new DBT will take time and resources, as well as new ways of doing business, sound management and leadership. Currently DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities against the new DBT. DOE and NNSA are developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated. However, the fiscal year 2006 budget will probably be the first to show the budgetary impact of the DBT. Once funds become available, most sites estimate it will take from 2 to 5 years to fully implement, test, validate and refine strategies for meeting the new DBT requirements."

The DOE report contains detailed descriptions of the vulnerability assessment process, computer modeling, protective force performance testing program, explosives detection program and technology, Design Basis Threat and adversary characteristics, risk management process through Site Safeguards and Security Plans (SSSP's) and the safeguards and security oversight program. While these safeguards and security process descriptions are generally accurate, the DOE report fails to provide evidence that these critical programs have been fully implemented and their effectiveness tested at the nation's nuclear weapons complex. A recent GAO report stated, "NNSA disagreed with the conclusion that it was not ensuring the comprehensive annual assessments of contractors' performance that DOE policy requires. NNSA believed that its surveillance activities were also comprehensive; however NNSA provided no evidence – such as implementation guidance to the sites that are conducting surveillances – that would ensure the sites' surveillance activities conform to DOE's policies." (GAO-03-471

Nuclear Security NNSA Needs to Better Manage Its Safeguards and Security Program; May 2003)

The DOE report has a detailed description of the SSSP process and describes it as the cornerstone of their risk management program. It is very interesting to note that the GAO also discovered significant problems in that area: "NNSA largely suspended the development of SSSP's pending the issuance of the new DBT."

The report also describes DOE's protective force performance testing program as one of the best. The DOE statement is misleading, because while DOE's performance testing program has the *capability* to be one of the best, at the time of my disclosure it was and continues to be grossly underutilized.

In fact, matters are deteriorating further in some areas. Performance tests using highly qualified military special operations personnel as adversaries have been discontinued since 9/11 and the overall number of performance tests has been reduced as well.

The GAO Testimony stated,

"For example, a recent DOE Inspector General report found that the large amounts of overtime needed to meet the higher SECON requirements have resulted in fatigue, reduced readiness, retention problems, reduced training and fewer force-on-force performance tests for the protective forces". (*Audit Report: Management of the Department's Protective Forces,* DOE/IG-0602, Department of Energy Office of the Inspector General, June 2003)

The DOE report also contains a lengthy and accurate discussion of the value of performance **exercises** for training. This is an irrelevant red herring. In performance exercises less skilled adversary teams can be effectively utilized and exercise evaluators can be trained. However, during performance **tests** adversary teams that are truly representative of terrorists and their capabilities, and fully trained and experienced evaluators must be used. DOE continues to conduct performance **tests** using adversaries that are not representative of the actual terrorist threat and some evaluators that are not fully qualified and use the results of **exercises** where **tests** are required. The bottom line is that the **exercises** provide only a shadow of the reliable data that is indispensable for an informed assessment of our defenses against terrorists.

The SSSP also must document the analysis that establishes the extent to which a facility explosives detection capability provides protection against the malicious use of explosives that could result in an unacceptable risk to public health or safety. SSSP's have not been completed and approved for all facilities in the DOE nuclear weapons complex. Although the DOE report has an elaborate description of the risk management process, it is silent on the issue of the actual status of SSSP's. Again, the Department leapfrogged the point of my disclosure.

DOE has access to world class protective force computer modeling capability through its network of national laboratories. Unfortunately DOE does not require that all protective force deployment strategies be evaluated using this highly effective tool and the standardized testing protocols necessary to ensure valid test results have not been developed. The current protective force deployment strategies at all nuclear weapons complex facilities have not been evaluated using computer modeling.

While it is acknowledged that some of the information contained in my whistleblower disclosure is dated and that DOE has made some security changes that are unknown to me, there is no mystery about the cornerstones of my charges: the status of SSSP's, level of utilization of military adversary teams for protective force performance tests and utilization of computer modeling for protective force evaluations is unclassified and readily available to me. I have done my homework from the available record and surveyed peers who are still in the field. The risk to national security assets entrusted to DOE continues to be unnecessarily and unacceptably high. **The current findings of the GAO summarized above clearly support my conclusion and significantly discredit the DOE report.** Many of the same deficiencies identified in my whistleblower disclosure were confirmed by GAO subsequent to the date of DOE's report, including inadequate comprehensive assessments/oversight; failure to manage deficiency resolution through corrective action plans and cost benefit analyses; a significant lack of staff expertise; and performance testing deficiencies that provide only uncertainty about the effectiveness of costly security measures; and, the inadequacy of the 1999 Design Basis Threat (DBT), the protracted period required to revise and issue the new DBT and the fact that DOE will not be in a position to fully address and mitigate the new threat for many years! In the topical areas reviewed by GAO virtually all of my deficiencies were validated.

DOE has acknowledged that the 1999 DBT is obsolete and issued a new DBT in May 2003. The GAO Testimony states,

"DOE's Office of Independent Oversight and Performance Assurance continued its inspections; however, it initially reduced the amount of force-on-force performance testing it conducted because of the high levels of protective force overtime caused by implementation of SECON level 2 and 3 measures. This Office also planned to begin performance testing at levels beyond the 1999 DBT, but has done so at only one site before the 2003 DBT was issued."

We know the 1999 DBT was rendered obsolete by the September 11 terrorist attacks. DOE had only conducted one performance test beyond the 1999 DBT prior to issuance of the May 2003 DBT. Thus the ability of the vast majority of DOE facilities to successfully defend against the terrorist threat issued in May 2003, which is acknowledged as highly credible, has not been thoroughly tested and validated, and is largely unknown. America's safety from terrorists remains indeterminate.

In conclusion, I continue to believe that the scope and magnitude of security problems at DOE, which were identified in my whistleblower disclosure, constitute a substantial and

specific danger to public health and safety. Given the significant increases in the terrorist threat which has been universally acknowledged since 9/11, the degradation of national security that results from these deficiencies is even greater now. I believe that any objective journeyman nuclear security professional evaluating my whistleblower disclosure, the GAO Testimony and the DOE report will find the DOE report seriously lacking in credibility, especially given the significant recent and directly conflicting GAO findings. I also believe the new information contained in the GAO testimony, i.e. that DOE will likely not have the financial resources necessary to address the May 2003 DBT until fiscal year 2006, and that it will take an additional 2 to 5 years to implement the required additional security measures, creates an extended window of vulnerability and exacerbates an already unsatisfactory situation. Given that DOE is protecting nuclear weapons and special nuclear materials and recognizing the catastrophic consequences associated with a security breach, only the highest level of protection is acceptable. Uncertainty about DOE's ability to protect nuclear weapons and special nuclear material is unacceptable. Until DOE abandons its longstanding approach of denial for any alleged security problems, our nation will continue to be vulnerable to preventable terrorist threats.

I appreciate the opportunity to review the DOE report. Please feel free to contact me at (301) 903-2178 if you or your staff has any questions.

Sincerely,

Original Signed by Richard J. Levernier

Richard J. Levernier

Attachment

3

United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

May 2003

NUCLEAR SECURITY

NNSA Needs to Better Manage Its Safeguards and Security Program

GAO-03-471

May 2003

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-03-471, a report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives

NUCLEAR SECURITY

NNSA Needs to Better Manage Its Safeguards and Security Program

Why GAO Did This Study

The attacks of September 11, 2001, intensified long-standing concerns about the adequacy of safeguards and security at four nuclear weapons production sites and three national laboratories that design nuclear weapons—most of these facilities store plutonium and uranium in a variety of forms. These facilities can become targets for such actions as sabotage or theft. The Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE—are responsible for these facilities. NNSA plays a crucial role in managing the contractors operating many of these facilities to ensure that security activities are effective and in line with departmental policy. GAO reviewed how effectively NNSA manages its safeguards and security program, including how it oversees contractor security operations.

What GAO Recommends

GAO is making four recommendations to the Secretary of Energy and the Administrator of NNSA to focus more on certain key management and oversight issues. Commenting on the draft report, NNSA disagreed with GAO's conclusion that NNSA was not ensuring the comprehensive, annual assessments of contractors' performance that DOE policy requires. GAO continues to believe that NNSA's current efforts do not ensure conformance to DOE policy.

www.gao.gov/cgi-bin/getrpt?GAO-03-471.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Robin M. Nazzaro at (202) 512-3841 or nazarror@gao.gov.

What GAO Found

NNSA has not been fully effective in managing its safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum advantage to protect critical facilities and material from individuals seeking to inflict damage. The four areas are as follows:

- *Defining clear roles and responsibilities.* NNSA still has not fully defined clear roles and responsibilities for its headquarters and site operations.
- *Assessing sites' security activities.* Without a stable and effective management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA sites on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities are subject to the comprehensive annual assessments that DOE policy requires.
- *Overseeing contractors' corrective actions.* To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or cost versus the benefit of taking corrective action.
- *Allocating staff.* NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for site offices to effectively oversee security activities.

Security Force in Action

Source: DOE.

Contents

Letter		1
	Results in Brief	4
	Background	7
	NNSA's Lack of Safeguards and Security Direction in Key Areas Results in Inconsistent Management of Contractors	9
	Conclusions	16
	Recommendations for Executive Action	16
	Agency Comments and Our Evaluation	17
Appendix I	**Comments from the National Nuclear Security Administration**	20
Appendix II	**GAO Contact and Staff Acknowledgments**	23

Abbreviations

DOE	Department of Energy
FRAM	*Functions, Responsibilities, and Authorities Manual*
NNSA	National Nuclear Security Administration

This is a work of the U.S. Government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. It may contain copyrighted graphics, images or other materials. Permission from the copyright holder may be necessary should you wish to reproduce copyrighted materials separately from GAO's product.

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 30, 2003

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Emerging Threats, and International Relations
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

Over the past decade, we and others have raised concerns about the adequacy of security at nuclear weapons facilities within the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE. For example, we reported in 2002 that DOE had not addressed problems in implementing security initiatives,[1] while an independent study by the Commission on Science and Security,[2] conducted at the request of DOE, found deficiencies in cyber security. Concerns over security within the nuclear weapons complex were brought into sharper focus by the September 11, 2001, terrorist attacks. These attacks highlighted the importance of effective physical security[3] in response to a potentially large and well-organized threat.

NNSA relies upon its safeguards and security program to ensure the physical security of the nation's nuclear weapons complex. Currently, the complex has four production sites: the Pantex Plant, Amarillo, Texas; the Y-12 Plant, Oak Ridge, Tennessee; the Kansas City Plant, Kansas City, Missouri; and the Savannah River Site, Aiken, South Carolina. In addition to the production sites, the complex includes the Nevada Test Site and three national laboratories that design nuclear weapons: Lawrence

[1] U.S. General Accounting Office, *Nuclear Security: Lessons to Be Learned from Implementing NNSA's Security Enhancements*, GAO-02-358 (Washington, D.C.: March 29, 2002).

[2] Commission on Science and Security, Center for Strategic and International Studies, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories* (Washington, D.C.: Apr. 2002).

[3] Physical security is the combination of operational and security equipment, personnel, and procedures used to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

Livermore National Laboratory, Livermore, California; Los Alamos National Laboratory, Los Alamos, New Mexico; and the Sandia National Laboratories, Albuquerque, New Mexico, and Livermore, California. To implement its safeguards and security program, NNSA relies on site contractors that are responsible for conducting day-to-day security activities and adhering to DOE policies as they operate the complex's laboratory and production facilities. The contractors' activities are subject to DOE-NNSA oversight. NNSA has offices—site offices—co-located with each site. Many of these sites possess Category I special nuclear material. Category I material includes plutonium and uranium in the following forms: (1) assembled nuclear weapons and test devices; (2) products containing higher concentrations of plutonium or uranium, such as major nuclear components, and recastable metal; and (3) high-grade materials, such as carbides, oxides, solutions, and nitrates. The risks this radioactive material poses vary, but include the potential for sabotage, or theft for illegal use in a nuclear weapon. Because these materials pose such risks, NNSA's management of the safeguards and security program, which includes overseeing contractor activities, is essential to preventing an unacceptable, adverse impact on national security.

DOE's Office of Security develops and promulgates orders and policies that guide NNSA's safeguards and security program. NNSA is responsible for ensuring that its contractors' security activities are effective and conform to DOE's orders and policy requirements. In conducting this oversight, NNSA generally uses certain key processes intended to identify specific weaknesses at contractor-operated sites and ensure that weaknesses are corrected. These processes include, among other things, (1) annual, comprehensive surveys conducted by subject matter experts from across the complex and (2) ongoing reviews of one or more aspects of contractors' program (surveillance) by NNSA site officials.[4]

DOE's Office of Independent Oversight and Performance Assurance also assesses contractor security activities. In response to NNSA surveys and assessments conducted by the Office of Independent Oversight and Performance Assurance, DOE policy requires contractors to prepare corrective action plans for identified problems and to ensure that these

[4] A surveillance is generally conducted by a single or small number of subject matter experts, and the documentation from a surveillance or group of surveillance activities may be used as part of the survey.

actions are based on documented root cause analysis, risk assessment, and cost-benefit analysis.

You asked us to review physical security at NNSA and DOE facilities that contain Category I materials. Specifically, as agreed with your office, this report examines how NNSA manages its safeguards and security program. This report is the first of two that we will be issuing to you on various aspects of physical security at NNSA and DOE facilities. Our followup report will focus on the extent to which physical security has improved; the effectiveness of the process for establishing safeguards and security requirements following the September 11, 2001, attacks; and the remaining vulnerabilities.

To evaluate the overall safeguards and security oversight process, we reviewed DOE policy and planning documents, including orders, implementation guidance, and reports. We looked at what the orders and guides prescribed, particularly DOE Order 470.1, and compared this to how operations and site offices were following and implementing the policies to see if there were any deficiencies. To determine how NNSA organizes and conducts overall safeguards and security oversight, we met with officials from DOE and NNSA headquarters and NNSA site offices. The primary offices from which we obtained information were from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and NNSA's Office of Defense Nuclear Security and Nuclear Safeguards and Security Program.[5] We also evaluated the NNSA reorganization with regard to the potential impact on oversight roles and responsibilities of NNSA headquarters and site offices.

We visited 7 site offices from March 2002 to October 2002, to determine how federal contractor oversight and the safeguards and security program is managed. Specifically, we visited Los Alamos National Laboratory and the Office of Los Alamos Site Operations in New Mexico, Sandia National Laboratory and the Office of Kirtland Site Operations in New Mexico, Department of Energy's Albuquerque Operations Office in New Mexico, the Office of Transportation Safeguards in New Mexico, Y-12 Plant, and the Y-12 Site Office in Tennessee, Pantex Plant and the Office of Amarillo

[5] We did not include naval reactors in our review because it is a semiautonomous entity within NNSA with a unique security structure and program.

Site Operations in Texas, the Savannah River Site[6] and the Savannah River Site Office in South Carolina, and Lawrence Livermore National Laboratory and the Livermore Site Office in California. At each location we met with both federal and contractor officials and obtained pertinent supporting documentation.

To determine how NNSA sites prepare and document corrective action plans and related analyses, we examined 43 closed and open corrective action plans dated from 1999 through 2002 that we selected at random from each of the 6 NNSA sites (as well as the DOE Savannah River Site, which is expected to come under NNSA's jurisdiction in the future) that contain category I special nuclear materials.[7] We reviewed these plans to determine the extent and type of analyses that support the corrective actions in the plans. These plans generally represent the contractors' actions to address high priority findings in contractors' security and safeguards program. To understand how the corrective action process currently works, we compared the processes in place at each NNSA site we visited during 2002.

We performed our review from December 2001 through April 2003 in accordance with generally accepted government auditing standards.

Results in Brief

NNSA has not been fully effective in managing its safeguards and security program in four key areas, and therefore, it cannot be assured that its contractors are working to maximum advantage to protect critical facilities and material from individuals seeking to inflict damage. The following four areas are key:

- *Defining clear roles and responsibilities.* Since its creation in March 2000, NNSA's management structure has been in a state of flux. While in December 2002, NNSA issued what it considers final directives for reorganizing headquarters and site offices, NNSA expects it will take until at least September 2004 to fully implement its new management structure. In particular, NNSA is still defining its site offices' roles and

[6] Although the Savannah River Site is still an Environmental Management designated site, according to site officials, it will likely become an NNSA site once the accelerated cleanup is complete. Because of its present role as a key DOE nuclear weapons production site, we included it in our review of site offices.

[7] One of the seven sites—Transportation Safeguards——is operated by NNSA, not a contractor.

responsibilities for safeguards and security. Specifically, it is still developing the components of a *Functions, Responsibilities, and Authorities Manual*, which will not be completed for several months because of the highly detailed planning necessary for determining staff functions at the various sites. This manual, which NNSA itself recognizes as crucial, is intended to set out roles and responsibilities clearly. This still-developing management structure led to confusion about the roles and responsibilities of the headquarters and site offices.

- *Assessing sites' security activities.* Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among the NNSA sites on how to conduct key aspects of safeguards-and-security assessment activities. In particular, three out of the seven NNSA site offices use the traditional survey approach, as required by DOE policy, to oversee security activities, while four have discontinued surveys and instead rely on surveillance activities. The distinction between these two activities is important: A survey provides a comprehensive annual review, by a team of experts from throughout NNSA, of contractor safeguards and security and generally takes about 2 weeks. In contrast, surveillance relies on a single or small number of NNSA site officials overseeing one or more aspects of a contractor's safeguards and security activities throughout the year. However, officials from DOE's Office of Security—which developed the policy for conducting surveys—believe the surveillance model does not comply with the DOE order because it does not provide a comprehensive overview. Furthermore, officials from DOE's Office of Independent Oversight and Performance Assurance and NNSA headquarters expressed concern about the site offices' ability to conduct surveillance because of shortfalls in available expertise. The four site offices have been able to operate using only surveillance activities because, during the reorganization of the management structure, NNSA has not issued guidance on complying with DOE policy for conducting surveys.

- *Overseeing contractors' corrective actions.* NNSA contractors do not consistently conduct the analyses DOE policy requires in preparing corrective action plans, compounding the problems in ensuring physical security. Inconsistency occurs because the NNSA site officials do not have implementation guidance from headquarters on how to address corrective actions. Of the 43 corrective action plans we reviewed for 1999 through 2002, less than half showed that the contractor had performed the required root cause analysis. Furthermore, less than 25 percent demonstrated that the contractor had performed a required risk assessment or cost-benefit analysis. As a

result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or cost versus benefit of taking corrective action. However, at the 7 sites we visited in 2002, the site offices and contractors are making some progress to establish formal processes for root cause and other analyses. Nevertheless, inconsistencies remain regarding the approaches used to complete these analyses. For example, some site processes specify that root cause analyses will be conducted for all corrective action plans, while other sites consider the completion of these analyses optional. An NNSA headquarters official stated that the agency expects to issue additional guidance for implementing DOE security policies in 2003.

- *Allocating staff.* NNSA has shortfalls at its site offices in the total number of staff and in areas of expertise, which could make it more difficult for the site offices to oversee safeguards and security effectively and to ensure that the agency fully knows security conditions at its sites. According to officials at 5 of the 7 site offices we visited, they have, or expect to have, an average of 2 to 6 vacancies per site for overseeing contractors' safeguards and security; typically, each site expects to have 10 to 14 security-related positions within the next 2 years. The vacancies occur, in part, because staff are reluctant to move to locations they view as less desirable and because NNSA has frozen hiring in response to budget constraints. Some of these vacancies are for specialists in particular subject areas, such as Industrial Security Systems—a key specialty needed for conducting physical security inspections. The lack of expertise and staff could be further complicated for some sites by NNSA's realignment plan. Under this plan, NNSA expects to streamline federal oversight of contractors and reduce headquarters and field staff by 20 percent by the end of fiscal year 2004. Site officials said that they will fill some vacancies through a virtual organization in which experts at other locations will assist with certain components of the surveillance activities. However, it will take time to work through some of the difficulties associated with making the transition to this approach.

We are making recommendations to the Secretary of Energy and the Administrator of the NNSA that are intended to place additional focus on key management and oversight dimensions during NNSA's ongoing reorganization.

In commenting on our draft report, NNSA concurred with two of our four recommendations, disagreed with one, and did not indicate agreement or disagreement with the fourth. NNSA concurred with our recommendation

to formally establish roles and responsibilities, and it plans to issue a formal document in 2003. NNSA also concurred that corrective action plans must be prepared in accordance with established standards and policy. NNSA disagreed with the conclusion that it was not ensuring the comprehensive annual assessments of contractors' performance that DOE policy requires. NNSA believed that its surveillance activities were also comprehensive; however, NNSA provided no evidence—such as implementation guidance to the sites that are conducting surveillances—that would ensure that the sites' surveillance activities conform to DOE's policies. Finally, regarding our recommendation that NNSA develop and implement a plan for effectively allocating staff for safeguards and security oversight, NNSA commented that managers have staffing plans and that its virtual organization and additional hiring will address sites' need for certain types of skilled personnel. In our view, while reliance on the virtual approach may be effective in the short term, the continuing vacancies at some sites indicate that NNSA may have difficulty attracting and retaining necessary expertise at specific, understaffed locations over the long term.

Background

Since its creation in 1977, DOE has been responsible for developing, producing, and maintaining nuclear weapons; preventing the proliferation of weapons of mass destruction; designing, building, and maintaining naval nuclear propulsion systems; and ensuring the security of the nuclear weapons complex. In 2000, however, the Congress created a separately organized agency within DOE—the NNSA.[8]

NNSA's Office of Defense Nuclear Security is primarily responsible for developing the agency's security programs, including protecting, controlling, and accounting for material and ensuring physical security for all facilities in the complex. Historically, NNSA has conducted comprehensive annual surveys of contractors' operations for safeguards and security. These surveys, which can draw upon subject matter experts throughout the complex,[9] generally take about 2 weeks to conduct and cover 5 "topical" areas and 32 subtopical areas. The topical areas include

[8] National Defense Authorization Act for Fiscal Year 2000, Pub. L. No. 106-65, tit. 32 (also known as the National Nuclear Security Administration Act).

[9] The core skill sets needed to address the safeguards and security elements at a facility include program management and planning; protective force operations; classified matter protection and control; physical security; technical security and security systems; nuclear material control and accountability; and safeguards and security program infrastructure.

program management, protection program operations, information security, nuclear materials control and accountability, and personnel security. The survey team assigns ratings of satisfactory, marginal, or unsatisfactory. Currently, NNSA's facilities have been rated satisfactory in most topical areas. All deficiencies (findings) identified during a survey require the contractors to take corrective action, and both findings and corrective actions are to be entered in the Safeguards and Security Information Management System—a DOE-wide, integrated tracking database for findings of surveys and other safeguards and security activities.

In addition, NNSA's Office of Facilities and Operations is expected to provide policy guidance for safeguards and security. This office is also expected to be responsible for the Nuclear Safeguards and Security Program, which oversees the implementation of safeguards and security in NNSA facilities. The office is expected to integrate and defend the budget for safeguards and security to ensure that program components can achieve mission objectives. Through various contract mechanisms, NNSA provides financial incentives, such as award fees, for contractor performance. NNSA assesses this performance based on the extent contractors meet a set of measures, which are generally established in annual performance plans—so-called performance measures.

DOE's Office of Independent Oversight and Performance Assurance supports NNSA in safeguards and security assessments and conducts independent oversight activities in line with DOE and NNSA policies and priorities. Among other things, the office is responsible for evaluating the effectiveness of contractors' performance in safeguards and security. To carry out this function, this office periodically assesses both federal and contractor operations at a site and identifies findings, issues, and opportunities for improvement. It also performs follow-up reviews to ensure corrective actions are effective and that weaknesses in safeguards and security are appropriately addressed.

NNSA's Lack of Safeguards and Security Direction in Key Areas Results in Inconsistent Management of Contractors

NNSA has not been fully effective in managing its safeguards and security program in four key areas, and therefore, it cannot be assured that its contractors are working to maximum advantage to protect its sites. First, NNSA has not fully defined safeguards and security roles and responsibilities. Second, without an effective management structure, site offices are uncertain about how to conduct their safeguards and security responsibilities. This uncertainty has resulted in inconsistencies in how site offices comply with DOE orders in assessing contractors. Third, even when assessments are done, NNSA contractors do not consistently conduct required DOE analyses in preparing corrective action plans. Finally, NNSA's shortfalls at its site offices in the total number of staff and expertise could make it more difficult for the site offices to oversee safeguards and security effectively.

NNSA Has Not Clearly Defined Roles and Responsibilities, Resulting in Confusion at Sites

Since its creation in March 2000, NNSA's management structure has been in a state of flux, and NNSA expects it will take at least to September 2004 to implement a new management structure. However, NNSA needs a stable structure to establish clear roles and responsibilities for its headquarters and site offices, including safeguards and security oversight. In May 2001, NNSA's Administrator proposed a management structure for his organization,[10] but in December 2001, we reported that a clearly delineated overall management structure still did not exist.[11] In February 2002, NNSA reported in more detail to Congress on its outline for a new management structure[12] to improve NNSA's effectiveness and efficiency. NNSA expected to implement the new structure later in the year.

Since then, NNSA headquarters and field officials have been defining safeguards and security roles and responsibilities. In December 2002, NNSA fundamentally changed the management structure for safeguards and security. It abolished operations offices, which had been responsible for conducting the annual, comprehensive surveys as well as other

[10] National Nuclear Security Administration, *Report to Congress on the Plan for Organizing the National Nuclear Security Administration* (Washington, D.C.: May 3, 2001).

[11] U.S. General Accounting Office, *NNSA Management: Progress in the Implementation of Title 32*, GAO-02-93R (Washington, D.C.: Dec. 12, 2001).

[12] National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the National Nuclear Security Administration* (Washington, D.C.: Feb. 25, 2002).

safeguards and security activities. It divided these operations offices' responsibilities among the site offices and a service center, formerly the Albuquerque operations office; headquarters will oversee the performance of the site offices. The restructuring brings day-to-day federal oversight of laboratories and plants closer to the site offices. However, these changes do not complete the management structure. NNSA plans to further streamline its oversight of contractors by reducing site activities. Among other things, NNSA plans to focus more on ensuring that contractors' management systems are valid. Furthermore, NNSA plans to review its policies and practices and decide which site office oversight activities can be reduced or eliminated in order for the site offices to work more efficiently. It has not yet identified which specific activities will be modified. At the time of our review, headquarters could not provide details on how it intends to monitor the NNSA site offices' performance with respect to safeguards and security or address deficiencies.

In creating this new management structure, NNSA has not yet developed a *Functions, Responsibilities, and Authorities Manual* (FRAM), an organizational tool used by managers at federal agencies, including DOE, for defining roles and responsibilities. This manual is to address the functions, responsibilities, and authorities of all elements within NNSA. NNSA headquarters security officials agree that this guidance is crucial and stated that they are currently developing the components of a FRAM, which should be finalized in 2003. NNSA told us that completing the FRAM takes significant time because of the highly detailed planning necessary for determining staff functions at the various sites.

According to NNSA site office officials, as they wait for formal guidance from headquarters on conducting security oversight, each office is carrying out oversight activities as it deems appropriate. In addition, these officials told us that they have not received formal notification about the change in their safeguards and security oversight responsibilities, such as responsibilities for the survey program. Officials at several site offices expressed frustration with this lack of direction.

NNSA's Security Assessment Processes Differ among Sites and Are Inconsistent with DOE Requirements

NNSA site offices are not consistent in how they assess contractor safeguards and security activities, and they may not be conducting these assessments in accordance with DOE policy. The lack of consistency and the failure to implement DOE policy occurs in part because the site offices have had to assume new oversight responsibilities without, among other things, clear guidance from headquarters on how to carry out these responsibilities. As a result, three offices of the seven NNSA site offices we

visited continue to use the traditional survey approach to oversee security activities (Oak Ridge, Savannah River, and NNSA's Office of Transportation Safeguards), while the remaining four have adopted or are adopting a surveillance model—Amarillo, Kirtland, Livermore, and Los Alamos. The distinction between these two activities is important: A survey provides a comprehensive annual review, by a team of experts, of contractor safeguards and security and generally takes about 2 weeks; formerly, the operations offices generally conducted surveys, assisted by experts from throughout the complex, as necessary. In contrast, surveillance relies on a single or small number of NNSA site officials overseeing one or more aspects of a contractor's safeguards and security activities throughout the year, and the documentation from a surveillance or a group of surveillance activities may be used as part of the survey.

By relying on surveillance, NNSA may have less assurance that it fully knows the condition of security at its sites and therefore potentially cannot act to correct deficiencies undisclosed by this limited review. Surveillance allows subject matter experts at the sites to evaluate areas of contractor safeguards and security performance more often than the traditional survey process and therefore potentially identify deficiencies faster. However, according to DOE officials, reliance on surveillance is not consistent with DOE orders calling for a comprehensive survey of a contractor's safeguards and security performance. This survey provides a unified assessment of all security-related topical areas.[13] Officials from DOE's Office of Security—which developed the policy for conducting surveys—believe the surveillance model does not comply with DOE order survey requirements because it is not comprehensive. Officials from DOE's Office of Independent Oversight and Performance Assurance expressed concern about the site offices' ability to conduct surveillance because of shortfalls in available expertise. Furthermore, the director of NNSA's Office of Defense Nuclear Security acknowledged that although some NNSA site offices, such as the Los Alamos site office, are using the surveillance model, this site and others lacked the necessary personnel to conduct surveillance.

According to officials from DOE's Office of Independent Oversight and Performance Assurance and one site office, surveillance is not compatible with the current Safeguards and Security Information Management

[13] The frequency of survey schedules can be modified if the site being surveyed meets certain criteria.

System, a DOE information database system used to track findings and associated corrective actions, and therefore could pose problems for sites in entering information. On the other hand, NNSA officials at site offices and headquarters argue that using the surveillance model for oversight will produce an annual end of the year survey report and should have the same end result as an annual survey. However, NNSA could have difficulty ensuring consistent and comprehensive assessments because of the difficulties posed by using the surveillance model without appropriate NNSA-wide implementation guidance, site office staffing shortfalls, and database compatibility problems.

NNSA's Corrective Action Practices Are Inconsistent with DOE Requirements

Contractors have not consistently prepared effective, formal root cause analyses in developing corrective action plans for identified deficiencies, as DOE policy requires.[14] An effective, formal, root cause analysis can enhance the development of corrective actions, as we observed while reviewing some plans. However, less than half of the 43 corrective action plans we reviewed, dated between 1999 and 2002, showed that the contractor had performed the required root cause analysis. Furthermore, in a few cases corrective action plans were based on root cause analyses that were poorly prepared, resulting in confusion and contradictions. For example, NNSA had identified a deficiency at one site of potential entry into a critical facility. The contractor did not fully develop a root cause for this problem but merely rebutted the finding's validity. Nevertheless, the contractor took a corrective action in response to this deficiency—spending about $150,000. However, because the root cause analysis was not fully developed, we could not determine how, or if, the contractor's corrective actions would correct the deficiency. Furthermore, the contractor's staff preparing the analysis did not have formal training in how to conduct root cause analyses. NNSA site officials agreed that the root cause analysis was performed incorrectly and that their oversight review of the analysis had not detected this problem.

Despite the problems some contractors have had in preparing root cause analyses, corrective action processes in 2002 at all 7 sites showed that some sites are making progress. For example, in late 2000, the Office of Transportation Safeguards, which is responsible for securely transporting critical NNSA items and material, had begun to correct significant weaknesses in its process for preparing and tracking corrective actions.

[14] DOE Order 470.1 Safeguards and Security Program; Sept. 28, 1995.

According to an official responsible for corrective actions at the office, the new process has already resulted in documented improvements to the quality and completeness of its corrective action plans. For example, the new process for root cause analyses identified additional reasons for a recurring NNSA finding on problems in how three federal agent facilities in NNSA's Office of Transportation Safeguards inspected the vehicles used to transport critical materials across the nation. These inspections are crucial in preventing individuals from attaching explosives or other foreign devices to the vehicles in potential attempts at sabotage or theft. The new process enabled NNSA to identify specific actions to ensure consistent interpretation and implementation of vehicle inspection procedures among the three facilities. Because the finding has not been repeated since July 2000, it appears that the additional corrective actions proved effective. Another site, Sandia National Laboratories, has developed a process for root cause analysis that other sites may find useful. Sandia uses a designated root cause analyst to systematically lead teams of subject matter experts at the laboratory through the steps for determining root cause. With this expert in root cause analyses, Sandia helps ensure that these analyses are consistent and effective.

Other analyses and assessments that are critical to planning corrective actions are also not consistently prepared at NNSA sites. In particular, less than 25 percent of the corrective action plans we reviewed showed documentation of other analyses required by the DOE order for corrective action, such as risk assessment or cost-benefit analysis. Without this documentation, we found it difficult to determine what process, if any, the sites had used to determine the risk level of the problem or the cost and relative benefit of implementing corrective actions.

Consistency problems are likely to continue without effective NNSA guidance for corrective actions. For example, at four sites we visited, the sites either did not require a risk assessment and cost-benefit analyses or stated that they were optional, depending on the site's evaluation of the need for an analysis. However, the remaining three sites we visited required these analyses for all corrective action plans. This inconsistency resulted in part from differing interpretations of the DOE order governing corrective actions. As a result, NNSA cannot be assured that all contractors are considering the costs of corrective actions in conjunction with the risk posed or the potential benefits to be gained. NNSA officials at some sites stated that, without implementation guidance, the intent of the DOE order requiring these analyses can be interpreted differently from site to site, which contributes to the inconsistent practices we observed. Since we provided our draft report to NNSA in April 2003, it has sent a brief

guidance letter on corrective action plans to its site offices, clarifying its analysis and documentation requirements. An NNSA headquarters official stated that issuance of additional guidance for implementing DOE security policies is expected in 2003.

And finally, NNSA sites do not consistently measure all performance aspects of contractors' preparation of corrective action plans and may reward contractors simply for closing the finding on schedule. According to our review of performance measures concerning corrective actions, four of the six contractor-operated sites we visited had measures that were primarily based on whether the contractor met the schedule for completing corrective actions, not on whether and how well the contractor had performed the analyses.[15] The other two sites did not consider any corrective action performance measures in assessing contractor performance—not even the schedule. However, DOE guidance encourages sites to measure qualitative factors, whenever possible, to minimize the need to rely solely on schedule-driven measures.[16] Effective qualitative performance measures would essentially reflect how well the contractor completes root cause analyses, risk assessment, and cost-benefit analyses.

The lack of qualitative performance measures affects the quality of the correction plan. For example, in fiscal year 1999, DOE's Office of Independent Oversight and Performance Assurance criticized a site that had schedule-driven performance measures for poorly prepared corrective action plans. Out of the 50 plans reviewed for that site, 27 had inadequate root cause determinations, and 15 had corrective actions that were unlikely to fix the deficiency cited. The performance measures in place for this contractor in fiscal year 1999—and then again in fiscal years 2000 and 2001—did not reflect qualitative aspects of these analyses; instead, they were primarily focused on schedule-driven outcomes. Some contract provisions permit the contractor to forfeit some of the award fee based on other generic performance factors, such as "management failure." However, these generic provisions may not be fully effective in motivating contractors in all aspects of their corrective action performance because

[15] One site, the Office of Transportation Safeguards is federally operated and therefore performance award fees are not applicable.

[16] U.S. Department of Energy, *Guidelines for Performance Measurement*, DOE G 120.1-5 (Washington, D.C.: June 30, 1996).

these provisions are not explicitly focused on corrective action and are therefore not highly visible.

Difficulties in Allocating Staff Could Hinder Effective Safeguards and Security Oversight

NNSA's site offices have shortfalls in the total number of staff and in the expertise for effectively overseeing contractors, including covering all topical areas in the annual surveys. At five of the seven sites we visited, NNSA officials told us that they currently have, or will have, two to six vacancies in safeguards and security positions once NNSA fully implements its new management structure; each site believes that it needs from 10 to 14 security-related positions in order to carry out its oversight activities under NNSA's new organization. In particular, some of the site offices are experiencing difficulty in filling positions because some staff consider the site locations less desirable than others and because NNSA has instituted a hiring freeze. Some of these vacancies are for specialists in particular subject areas, such as industrial security systems—a key specialty needed for conducting physical security inspections. Officials in the Office of Independent Oversight and Performance Assurance concurred that NNSA's reorganization and the shifting of responsibilities to the site offices has the potential to weaken security oversight.

To offset the lack of some subject matter experts at sites, NNSA field officials indicated that they frequently rely on subject matter experts from headquarters or other site offices to cover site offices that do not have expertise locally. With only a limited number of subject matter experts in the complex, the sites have to coordinate oversight carefully. Coordination is particularly complicated at those sites that have switched to a surveillance model since they may have to rely on particular subject expertise that is only available during certain times.

NNSA's new management structure further complicates the problems in staff allocation. NNSA expects to reduce headquarters and field staff by 20 percent by the end of fiscal year 2004. In this restructuring, NNSA plans to share staff expertise, creating a "virtual" organization to cover the needs of site offices and other areas within the complex until a final move of personnel can be made. Headquarters officials told us that it may take 1 to 2 years to move the appropriate safeguards and security persons to the areas where they are needed. Until then, they expect the virtual organization to meet the complex's needs. The virtual organization will include subject matter experts whose knowledge will be needed throughout the nuclear weapons complex and not just at their current sites. Some of these experts will work from the service center or be detailed to site offices as needed. With competing demands for the

experts, it is unclear how they will successfully provide assistance to site offices in their surveillance processes. The assistance may be unavailable when needed since components of surveillance are ongoing and may span an entire year.

Conclusions

Without effectively managing its safeguards and security program, NNSA cannot be assured that its contractors are working to maximum advantage to protect its nuclear weapons sites. These sites may have critical materials that could be prime terrorist targets. Several factors contribute to this lack of assurance. NNSA continues to change its management structure, making it difficult to define roles and responsibilities clearly. Without a functional management structure, some site offices and contractors may not be carrying out their security responsibilities, as DOE orders require. In particular, NNSA has not fully assured itself that the four sites that rely on surveillance activities, rather than on the DOE-required surveys, are overseeing contractors' security activities in the integrated, comprehensive fashion that are called for in the annual surveys. Moreover, when NNSA site offices allow and reward contractors for closing findings without ensuring that the contractors have correctly identified the root cause, assessed risk, and conducted a cost-benefit analysis, NNSA cannot be assured that the security problem identified was adequately addressed. Finally, to provide effective oversight, NNSA needs to develop an approach, beyond its "virtual" organization, that ensures its limited security resources are able to provide oversight, over the long term, where and when it is needed.

Recommendations for Executive Action

In order to strengthen the safeguards and security program of the nuclear weapons complex, we recommend that the NNSA Administrator and Secretary of Energy

- formalize the roles and responsibilities of site offices and headquarters for conducting oversight;
- ensure that sites are performing oversight using a survey approach that provides an integrated comprehensive view of security conditions and is consistent with DOE orders;
- ensure that contractors' corrective action plans are prepared and documented consistently and are based on qualitative root-cause, risk-assessment, and cost-benefit analyses, and that appropriate incentives are used to help motivate contractors toward effectively addressing findings; and

- develop and implement a plan to ensure that NNSA allocates safeguards and security staff so that it provides effective safeguards and security oversight over the long term.

Agency Comments and Our Evaluation

We provided the DOE's NNSA with a draft of this report for review and comment. Overall, NNSA concurred with two of our four recommendations, disagreed with one, and did not indicate agreement or disagreement with the fourth. In the area of concurrence, NNSA concurred with our recommendation to formally establish roles and responsibilities, and it plans to do so in 2003. NNSA also concurred that corrective action plans must be prepared in accordance with established standards and policy and based on documented root cause analysis, risk assessments, and cost-benefit analysis. Since we provided our draft report to NNSA, it has sent its site offices a guidance letter on corrective action plans that clarifies its analysis and documentation requirements. NNSA now allows required elements to be omitted from corrective action plans, but only if the contractors document the rationale for the exclusion as a formal part of their plan. We believe this guidance letter is a positive step in clarifying some implementation aspects of the DOE requirements, and we encourage continued management attention to this area. NNSA did not comment on the portion of this recommendation concerning the use of appropriate incentives to motivate contractors to address findings effectively.

NNSA disagreed with the conclusion that led to our recommendation to conduct oversight using a survey approach, which provides an integrated, comprehensive view of security conditions and is consistent with DOE orders. Specifically, NNSA disagreed with our conclusion that it was not ensuring the comprehensive annual assessments of contractors' performance that DOE policy requires. As we reported, four of the seven site offices no longer conduct comprehensive, integrated surveys to assess security but instead rely on surveillance activities. NNSA believed that these surveillance activities were also comprehensive; however, NNSA provided no evidence—such as implementation guidance to the sites that are conducting surveillances—that would ensure that the sites' surveillance activities conform to DOE's policies. Without such guidance, NNSA cannot be fully assured that surveillance activities, as presently conducted, provide the comprehensive assessment DOE requires in its surveys. Our recommendation therefore is intended to focus NNSA management attention on ensuring that site offices conduct security assessments that are integrated, comprehensive, and on par with the survey approach previously used and currently described in DOE orders. Furthermore, NNSA asserted, incorrectly, that we found its security

posture to be at risk. Assessing NNSA's security posture was not the objective of this report. Rather, our objective was to assess the way NNSA manages its overall security program. We have clarified the report, where appropriate.

Finally, regarding our recommendation that NNSA develop and implement a plan to ensure that it effectively allocates staff to provide safeguards and security oversight, NNSA commented that managers have staffing plans and that its virtual organization and additional hiring will address sites' need for certain types of skilled personnel. Reliance on the virtual approach may be effective in the short term. However, the continuing vacancies at some sites indicate that NNSA may have difficulty attracting and retaining necessary expertise at specific, understaffed locations over the long term. NNSA's comments do not indicate that it fully understands the need to address this longer-term problem. We have modified our recommendation to target this specific long-term concern.

We modified our report, where appropriate, to reflect NNSA's comments and to clarify some of our conclusions. NNSA's comments on our draft report are presented in appendix I.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will send copies of the report to the Secretary of Energy, the Administrator of NNSA, the Director of the Office of Management and Budget, and appropriate congressional committees. We will make copies available to others on request. In addition, the report will also be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please call me at (202) 512-3841. Major contributors to this report are listed in appendix II.

Sincerely yours,

Robin M. Nazzaro

Robin M. Nazzaro
Director, Natural Resources
and Environment

Appendix I: Comments from the National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

APR 25 2003

Ms. Robin Nazzaro
Director
Natural Resources and Environment
U.S. General Accounting Office
Washington, D.C. 20548

Dear Ms. Nazzaro:

The National Nuclear Security Administration (NNSA) appreciated the opportunity to have reviewed draft report GAO-03-471, "Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program." While many of the recommendations can help to improve areas of security program management, we categorically disagree with the GAO's conclusion and implications in sections throughout the draft report that NNSA cannot be assured that it is protecting its nuclear weapons' sites.

The report addresses the structure to manage security and the methodology to carry out security review processes. It does not include any information or basis on which to make a judgment or inference regarding the effectiveness of the NNSA security programs and infrastructure. Numerous internal and independent external reviews, including rigorous force-on-force and in-depth analysis and evaluation of protection system effectiveness across all of the NNSA sites have verified that the security posture is and remains strong and effective. We urge you to edit the document, including its proposed title, to appropriately reflect this.

A central focus of NNSA, since its establishment, has been to improve management of its programs. During the period of time that the draft GAO report was being developed, NNSA has made significant progress not only in the structure of the safeguards and security organization, but throughout the entire organization. Our lines of authority have been strengthened to provide accountability at all levels of the NNSA. Our business practices reflect the new management philosophy to achieve effective efficiencies that include implementing "best practices" or changing long-standing, less efficient processes. An example of this philosophical change is GAO's discussion of security surveillance versus security surveys. The NNSA management model is designed to streamline oversight, increase governmental efficiency, and provide greater management flexibility to contractors, while maintaining accountability. The surveillance methodology is only one of a number of assessment mechanisms that can be used to help assure timely understanding of security system performance as well as procedural compliance.

The GAO's recommendation on formally establishing roles and responsibilities under the new NNSA management structure is appropriate. A draft functions,

Printed with soy ink on recycled paper

responsibilities and authorities document reflecting the recently announced NNSA reengineering, has been put together and will be finalized with the NNSA field activities this year. However, it is very important that GAO also acknowledge that there is a sixty-year base of safeguards and security program policies, orders, implementation and organizational roles and responsibilities. This was not suspended on the stand-up of the NNSA or in the recently announced reengineering in late December 2002. It is this very base of safeguards and security programs and operations on which NNSA now, through its reengineering efforts, is working to further improve the effectiveness and efficiency of its safeguards and security and all other program activities.

NNSA disagrees with the conclusions in the GAO report regarding the appropriate manner in which site security activities are assessed and the comprehensiveness of those assessments as it applies to Security Surveys versus Security Surveillances. We do no fully agree with the comment that "...NNSA sites that rely on surveillance activities, rather than the DOE required surveys, are not overseeing contractors' security activities in the integrated comprehensive fashion that the annual surveys call for." Surveillances are only a part of the planned oversight and evaluation activities. A vital element of a surveillance program is the scoping of the topical and sub-topical elements to ensure that a comprehensive review of the critical program elements will be accomplished during the surveillance cycle. Areas not addressed in the current surveillance cycle are automatically included in the next cycle. When completed, a comprehensive report incorporating all surveillance activities of the safeguards and security program, including findings and observations, is forwarded to Headquarters. Regarding the adequate staffing of comprehensive surveillances, effective use of matrix support between NNSA site offices and support service contractors has afforded the use of well-qualified subject matter experts for the conduct of surveillance activities.

NNSA agrees with the GAO that corrective action plans must be prepared, implemented, and evaluated through resolution. We also agree that the causal effect must be established and addressed. This can be achieved by root-cause analysis or risk assessment with the accompanying cost-benefit analysis when appropriate. A guidance letter on this issue has been sent to NNSA activities by the Chief, Defense Nuclear Security, this week. With a continual contractor performance evaluation system supplemented by Federal oversight, NNSA will achieve a level of confidence that corrective action plans are appropriately developed and closed in a timely, and cost-effective manner. Please be assured that the focus of the NNSA is on effective safeguards and security performance. Oversight is a tool that is used to identify opportunities for improvement Additionally, NNSA Headquarters, through Policy Letters or other means, will provide the NNSA specific guidance for all programmatic and business functions. An example of this process is evidenced by the draft Policy Letter, "NNSA Line Oversight and Contractor's Assurance System."

The size of the Federal staff within NNSA is being reduced. As part of the re-engineering effort, each Site Manager, the Service Center Manager, and the Deputy/Associate Administrators have prepared staffing plans for their specific areas of responsibility. Safeguards and security is an important part of this NNSA effort. Where critical vacancies exist; hiring, support from the service center, other site offices and/or headquarters are all available options to assure each NNSA site has the appropriate skills mix to effectively execute their safeguards and security program assessment responsibilities. Finally, while the draft report references comments from the Department of Energy's Office of Independent Oversight and Performance Assurance regarding the potential to weaken security oversight if staffing and expertise at site offices are not addressed; they have also stated that NNSA's reorganization steps, to date, have helped to clarify roles and responsibilities for security oversight and that future plans have the potential to further strengthen security oversight.

We would welcome the opportunity to meet with the GAO staff that prepared the draft report in order to expand on the above comments and link them to the specific areas of the draft report.

Sincerely,

Anthony R. Lane
Associate Administrator
for Management and Administration

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

James Noel (202) 512-3591

Acknowledgments

In addition to the individual named above, Christopher R. Abraham, Jill Berman, Jonathan M. Gill, Andrea R. Miller, Christopher M. Pacheco, and Carol Herrnstadt Shulman made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:

Voice:	(202) 512-6000
TDD:	(202) 512-2537
Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

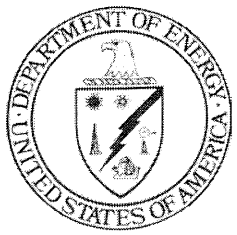
Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

4



U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Management of the Department's Protective Forces

DOE/IG–0602 June 2003

Department of Energy
Washington, DC 20585

June 3, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of the Department's Protective Forces"

BACKGROUND

The Department of Energy and its contractors are responsible for protecting materials and facilities critical to the Nation's nuclear defense program, as well as those used to support scientific, research, and environmental-related missions. While the security of Department sites has been a priority for many years, in the wake of the terrorist attacks of September 11, 2001, the Department took action to enhance security at its facilities. One important aspect of this initiative was an increased need for additional protective force personnel. For example, at National Nuclear Security Administration sites, authorized positions increased by 17 percent, to 2,319 officers. Once all positions are filled, annual security force costs for those sites are expected to exceed $251 million for the current fiscal year, an increase of 67 percent.

In previous reports, the Office of Inspector General identified a number of efficiency concerns relating to the Department's management of its protective forces. In light of these concerns, we initiated this audit to evaluate the Department's management of its protective force program.

RESULTS OF AUDIT

Our review disclosed that in the post-September 11 period, a number of improvements had been made in the management of the protective force program. However, we noted that the Department still faced a number of challenges that could adversely affect the program. Specifically, we observed:

- Long delays associated with granting clearances for newly employed protective force officers;
- Significant increases in unscheduled overtime costs;
- Morale and potential retention problems based on mandatory overtime and declining training opportunities; and,
- Operational vulnerabilities associated with unscheduled work stoppages.

Printed with soy ink on recycled paper

Clearly, the Department, like other Government agencies, faced a number of challenges relative to the unanticipated demand for supplemental security forces immediately after September 11, 2001. Now, however, the Department has the opportunity to improve the operation of its protective force program by taking advantage of accelerated methods of processing security clearances for officers, implementing related contractor performance expectations, and developing an overall protective force contingency strategy. Implementation of these measures should enhance management of the protective force, ultimately reduce costs for mandatory overtime, and help ensure that sensitive national defense and other mission-related facilities are appropriately protected.

We noted that the Department had already taken a number of actions to reduce the impact of heightened security on overtime costs. For example, the National Nuclear Security Administration (NNSA) issued guidance granting authority to arm protective force personnel who have "L" – rather than the higher level "Q" – clearances to help alleviate overtime costs and free up officers to attend required training sessions. NNSA also initiated a study to determine how to decrease unscheduled overtime to an acceptable level. Additionally, the Department has begun the process of hiring approximately 400 more officers to reduce unscheduled overtime.

While these are positive steps, additional action is needed to improve the Department's protective workforce. Consequently, we made a number of recommendations to develop and implement workforce management tools that should assist the Department and its contractors in maintaining an effective security force.

MANAGEMENT REACTION

Management generally concurred with our recommendations regarding accelerated clearance processing, workforce monitoring, and overtime. While most Department organizations endorsed the need for an agency-wide contingency plan, one office stated that such a plan was impractical and recommended that only site-level plans be developed. Overall, management has implemented, or intends to implement, actions that should satisfy our recommendations. Management's comments are included verbatim in Appendix 3.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration, NA-1
Under Secretary for Energy, Science and Environment
Director, Office of Security, SO-1

MANAGEMENT OF THE DEPARTMENT'S PROTECTIVE FORCES

TABLE OF CONTENTS

Protective Force Concerns

Details of Finding 1

Recommendations and Comments 5

Appendices

1. Objective, Scope, and Methodology 7
2. Prior Reports 9
3. Management Comments 10

MANAGEMENT OF THE DEPARTMENT'S PROTECTIVE FORCES

Protective Force Concerns

Although the Department of Energy (Department) had taken steps to improve the management of its protective forces, it faced a number of challenges that included delays in processing security clearances, increasing overtime costs, potential retention problems, and operational vulnerabilities associated with unscheduled work stoppages.

Security Clearance Processing

Even though the Department had initiated a number of efforts to increase the population of fully qualified protective force officers, security officials told us that these efforts have not been completely effective because of long delays associated with security clearance processing. According to security officials at Los Alamos, newly hired officers were not available for assignments requiring a "Q" clearance for as long as a year and a half while their clearances were being processed through routine channels. As of December 2002, a National Nuclear Security Administration (NNSA) management official told us that nationwide, 22 percent of NNSA's security officers (over 400 individuals) were not available to assume some or all of their duties because of problems and delays in processing security clearances.

Overtime Costs

Qualifying officers in a timely manner for assignment is critical because it directly affects the overall cost of security for the Department. The increase in security posture and the corresponding need for fully qualified officers, coupled with long clearance processing times, have caused overtime costs to increase significantly since September 11th. For example, since the terrorist attacks, Pantex has incurred an additional 281,739 overtime hours at a fully burdened cost of $13,253,180. Also, Sandia has incurred an additional 41,080 overtime hours annually, equating to $2,083,000 per year, in overtime. Officials at the Nevada Test Site indicated that they have experienced an 11 percent increase in overtime at an unburdened cost of $425,000. While increases are likely to be similar at other sites, we were unable to develop estimates because the Department did not always track mandatory overtime costs.

Morale and Retention Issues

In addition to cost considerations, increases in unscheduled overtime and a resulting decline in training opportunities may adversely impact

the ability to retain qualified officers. For example, we recently reported[1] that one site that had significant amounts of overtime, had not ensured the conduct of mandatory refresher training, and was experiencing high attrition rates. Since the change in security posture, heavy burdens associated with mandatory overtime have significantly reduced the availability of fully qualified officers for training. Morale suffered because certain officers have been unable to advance and have been denied vacations. In an effort to address these issues, NNSA told us that after September 11, 2001, it initially provided relief by adjusting training requirements.

While the training adjustments initially ameliorated operational impacts, they did not completely resolve morale and effectiveness problems. For example, at certain locations, officers were denied vacations, filed complaints because of what they characterized as "excessive" overtime, and in some cases, were unable to advance because they could not obtain necessary specialized training. Contractor officials at certain sites also indicated that the inability to attend training could become an attrition issue, and without relief, may lead to increased losses. While supervisory security management officials believed that losses may have occurred because of overtime and training issues, they told us that they could not quantify the number of officer losses due to these issues because they did not track reasons for attrition. Site security officials explained that the opportunity to participate in training is important because it provides a break, or "refresher" period that in addition to the direct benefits, permits officers to refocus. NNSA officials told us that the issue could become critical because officers at three of nine NNSA sites were experiencing fatigue that could diminish their effectiveness. The actual or potential loss of fully qualified officers is significant because of the estimated $37,000 initial cost to train a replacement and the resulting increase in mandatory overtime that must be incurred by the remaining force.

Operational Vulnerabilities

The Department also had not developed a contingency plan and may not be adequately prepared to respond to potential protective force shortages caused by unscheduled work stoppages or the activation of military reserve forces. Even though individual sites had developed plans, they were primarily designed to provide minimum levels of protection for materials. According to site officials, such levels may

[1]The cited Office of Inspector General report is classified.

not be sufficient to allow sites to carry out production, testing, or other mission-related activities in the event of a protective force strike. The significance of the problem could be exacerbated by the fact that four major site contracts expire and must be renegotiated within a ten-month period. If shortages of officers occurred at several locations simultaneously, the Department could be forced to shut down critical operations at those sites. Site level plans also do not specifically address supplementing protective forces with officers from other sources in the event of the activation of military reserve forces. The impact of such recalls could be substantial because military reservists at Lawrence Livermore, Sandia, and Los Alamos comprise 13.7, 10.9, and 14.6 percent, respectively, of the workforce.

Opportunities for Improvement

While the Department was initially unable to immediately respond to shortages of protective forces, it now has the opportunity to improve protective force management. Specifically, the Department had not taken advantage of accelerated methods of processing security clearances for officers, implemented related contractor performance expectations, and established responsibility for and developed a cooperative Department-wide protective force contingency plan.

Accelerated Clearance Processing

Several sites had not taken advantage of clearance processing options to mitigate cost and workforce impacts associated with the change in security posture. For instance, Sandia National Laboratories did not fully utilize the Department's Accelerated Access Authorization Program (AAAP) to minimize the period new employees were assigned to "restricted duties." The AAAP expedites the security clearance process by granting a "Q" interim access authorization and allows the officer to begin working with classified material before the standard background investigation is complete. Some sites also did not use prescreening techniques such as credit and local agency checks to help expedite the qualification process. In contrast, Pantex and the Nevada Test Site utilized an accelerated process and were able to fully utilize new officers up to six months sooner. Pantex and the Nevada Test Site also routinely prescreened applicants to decrease the risk of rejection and speed the clearance grant. Headquarters officials in the Office of Security told us that even though the accelerated process had been in

place for a number of years, some sites chose not to take advantage of it. While costs of the program and prescreening were $500 to $1,000 higher than routine processing, officials at Pantex indicated that the benefit of having officers available for unrestricted assignment significantly outweighed the cost of the accelerated program.

Contractor Performance Expectations

A lack of contractor performance expectations may also have affected the Department's ability to reduce overtime costs. For example, most sites did not include in their contracts a performance expectation that the contractor would evaluate cost effective alternatives to overtime. In fact, only Pantex included a Fiscal Year (FY) 2000 performance expectation that the contractor would develop alternative methods to reduce protective force overtime. Of the four sites we visited, Pantex had acted the most aggressively in reducing clearance-processing time and had the lowest current percentage of overtime. Incorporating security performance expectations into operating contracts could incentivize contractors to improve performance and would provide the Department with a mechanism to potentially reduce protective force costs.

Contingency Planning

The Department had not assigned responsibility or authority for developing and implementing a complex-wide protective force contingency plan. Currently, responsibility for protective force resources is distributed across organizational lines and no effort has been made to coordinate an overall plan. For example, Office of Security officials believed that it was not feasible for them to develop a plan because they had neither the responsibility to develop nor the authority to implement such a plan. An NNSA official, on the other hand, believed that a plan was needed and that it could involve actions such as developing formal memorandums of understanding with military or Federal law enforcement agencies. Without an inclusive plan, the Department may not be adequately prepared to respond to potential protective force shortages caused by unscheduled work stoppages or the activation of military reserve forces.

Operational Impacts

Unless actions are taken to address overtime and related issues and develop an organization-level contingency plan, the Department risks reducing the effectiveness of its protective forces and its ability to

adequately protect sensitive nuclear or other national defense related facilities. Specifically, continued high levels of stress caused by excessive overtime increases physical fatigue and could evolve into health and safety issues for the Department. Additionally, the Department faces potential increases in protective force attrition caused by overtime-induced stress and fatigue.

Furthermore, if unanticipated events such as strikes or significant military recall were to occur, the Department may not be able to obtain a sufficient number of replacement security officers. For example, at Pantex, officials notified Headquarters of a possible strike and requested approximately 100 replacement officers based on their minimum need. However, Headquarters lacked a Department-level plan or agreements with sites and was only able to secure about 25 replacement officers through ad hoc requests for volunteers from other locations. Because of the lack of centralized support, Pantex officials were forced to bargain, through their site contacts, for the additional officers necessary to sustain minimum nuclear material protection needs. The lack of labor distribution data also limited the ability of site and program officials, such as those from NNSA, to monitor or control mandatory overtime costs.

RECOMMENDATIONS

We recommend that the Administrator, National Nuclear Security Administration and the Under Secretary for Energy, Science and Environment work together and take the following actions:

1. Increase the use of prescreening in conjunction with the AAAP to improve the timeliness of the clearance process;

2. Incorporate performance expectations into the Department's management contracts directed at the use of cost effective alternatives to administering protective force overtime costs;

3. Develop a Departmental level protective force contingency plan; and,

4. Track protective force overtime costs and attrition rates as a means to monitor the effectiveness of workforce management initiatives at the contractor and program level.

MANAGEMENT REACTION

We received comments from NNSA and from the Department elements reporting to the Under Secretary for Energy, Science and Environment.

Management generally agreed with the draft report and the recommendations. Regarding recommendation 2, management's written comments expressed concern that incorporating performance expectations focused on overtime costs would be counterproductive. Subsequently, we clarified that the intent of that recommendation was to encourage the use of available alternatives to overtime. Management concurred with recommendation 2 as now stated in the report.

While most organizations commenting believed it may be appropriate to develop a Department-wide contingency plan, some expressed concern that such a plan might not be practical. The Department's verbatim comments can be found in Appendix 3.

AUDITOR COMMENTS

Management's comments, including discussions held subsequent to receiving the written responses, indicated the Department's intent to take action that will satisfactorily address the recommendations. However, management has not yet prepared a formal corrective action plan.

Appendix 1

OBJECTIVE

To determine whether the Department was adequately managing its protective force program.

SCOPE

We conducted the audit from April 2002 to December 2002, at Department of Energy Headquarters in Washington, DC; Sandia National Laboratories in Albuquerque, New Mexico; Los Alamos National Laboratory in Los Alamos, New Mexico; Pantex Plant in Amarillo, Texas; and Nevada Test Site, in Las Vegas, Nevada.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed actions taken by the Department since the issuance of the audit report *Management and Cost of the Department of Energy's Protective Forces* (DOE/IG-0354, July 1994);
- Reviewed applicable Federal regulations, Departmental orders, and implementing procedures and practices at Headquarters and at four sites;
- Reviewed current union agreements at the four sites visited, as well as six other sites;
- Reviewed and analyzed protective force costs (labor, overtime, training, exercise program, and supplies and equipment);
- Obtained and analyzed Office of Security quarterly and yearly strength reports;
- Reviewed performance-related information to determine compliance with the Government Performance and Results Act of 1993;
- Held discussions with Headquarters and other Federal Government officials regarding the Department's protective forces; and,

- Held discussions with officials from Sandia and Los Alamos National Laboratories, as well as the Pantex Plant and Nevada Test Site regarding protective forces.

The audit was performed in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Accordingly, the assessment included reviews of Departmental and regulatory policies, procedures, and performance measures related to the Department's protective forces. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not conduct a reliability assessment of computer-processed data because only a very limited amount of computer-processed data was used during the audit.

The exit conference was held with management on May 6, 2003.

Appendix 2

PRIOR AUDIT REPORTS

OFFICE OF INSPECTOR GENERAL RELATED REPORTS

- *The Restructure of Security Services by the Oak Ridge Operations Office,* (DOE/OIG-0487, October 2000). The purpose of the audit was to determine why security costs increased at the Oak Ridge Reservation after the restructuring of its security services. The audit disclosed that the Oak Ridge Operations Office did not manage the restructuring effort in a way that would have achieved its goals. Specifically, the Operations Office did not perform an analysis of security service staffing levels, determine the scope of work to be transferred, or develop cost-reduction measures or incentives to ensure efficient contractor performance. In addition, the Operations Office did not consider cost as a ranking factor in the selection of security services. Management concurred with the finding and recommendations and agreed to initiate corrective actions.

- *Security Overtime at the Oak Ridge Operations Office,* (ER-B-00-02, June 2000). The purpose of the audit was to determine whether the Oak Ridge Operations Office's new security contract provided incentives for Wackenhut to reduce overtime and minimize costs. The audit found that the new contract did not provide Wackenhut with incentives to reduce overtime or minimize costs. This occurred because the Operations Office did not consider contractual incentives for overtime reductions to be necessary. As a result, the Department could incur a significant amount in avoidable overtime costs during the term of the contract. Management concurred with the finding and recommendations and agreed to initiate corrective actions.

- *Management and Operating Contractor Overtime Costs*, (DOE/OIG-0381, October 1995). The objective was to determine whether the Department had controls in place to monitor and manage contractor overtime use. An analysis of the 50 management and operating contracts that were in effect at the end of FY 1994 and a detailed review at four of these contractors showed that the Department did not adequately monitor and manage contractor efforts to minimize overtime. Management did not specifically concur or nonconcur with the finding and recommendations. Management commented that it had identified a need to implement an overtime policy that was consistent with contract reform initiatives and that balances the need for reduced oversight against the need to demonstrate responsible stewardship of taxpayer dollars.

- *Management and Cost of the Department of Energy's Protective Forces*, (DOE/IG-0354, July 1994). The purpose of the audit was to determine if protective forces were efficiently managed and appropriately sized in light of the changing missions and current budget constraints. The audit noted several opportunities for the Department to improve the operational efficiency of the protective forces operations, including eliminating overtime paid to officers prior to completion of the basic 40-hour workweek. Management concurred with the findings and recommendations and agreed to take appropriate actions to improve the efficiency of managing protective forces.

Appendix 3

Department of Energy
Office of Science
Washington, DC 20585
April 3, 2003

Office of the Director

MEMORANDUM FOR FREDERICK D. DOGGETT
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDIT SERVICES

FROM: RAYMOND L. ORBACH
DIRECTOR
OFFICE OF SCIENCE

SUBJECT: Comments on IG Draft Report, "Management of the Department's Protective Forces"

The Departmental Elements for the Under Secretary for Energy, Science and the Environment have reviewed the subject report and offer the following comments, which have been summarized from their original submittals.

We appreciate the insightful comments and recommendations of the IG. Generally, the recommendations in the report contained merit and the respective Departmental Elements are addressing the recommendations as appropriate.

Specific Departmental Element Comments:

The Office of Science (SC) provides the following input to the four recommendations made in the report:

1. Increase the use of prescreening in conjunction with the AAAP to improve timeliness of the clearance process.

   SC will emphasize the availability of the timely AAAP process as needed for SC sites that carry weapons (Oak Ridge National Laboratory (ORNL) and Brookhaven National Laboratory (BNL)). Extensive prescreening processes are in place to choose candidates for the AAAP process at ORNL.

2. Incorporate performance expectations into the Department's management contracts directed at administering protective force overtime costs.

   Performance Evaluation Plans for the protective services contractor (Wackenhut Services, Inc. - Oak Ridge (WSI-OR)) have routinely included Performance Objectives for the management of overtime. Contract administrators closely monitor overtime usage, and extensive effort is placed on overtime reduction by WSI-OR management. The overtime costs at BNL are within acceptable limits. This is a challenge when the Department SECONs go up and down.

Printed with soy ink on recycled paper

1. Develop a Department level protective force contingency plan.

   SC has read and commented on a draft DOE-wide plan (guidance only) for contingency forces from the Office of Security.

2. Track protective force overtime costs and attrition rates as a means to monitor the effectiveness of workforce management initiatives at the contractor and program level.

   These costs and rates are tracked at SC sites that carry weapons. Management and contract administrators will remain alert to any developing trends in this area and, as necessary, apply action to rectify any problems noticed.

The Office of Fossil Energy concurs with the IG findings and recommendations with the caveat that the use of departmental resources should be justified by cost benefit analysis and/or by human safety and health considerations, national security, etc.

As a general comment, the Office of Nuclear Energy, Science and Technology stated that since only NNSA sites were reviewed, there may be inaccuracies introduced in trying to extrapolate the audit results to the entire DOE complex. Specific comments:

1. Memo, page 1, sixth line of background section: Add "at various facilities" after the phrase "to one of denial."

2. Memo, page 1, second to last sentence: Change "qualifying" to phrase "processing security clearances for"

3. Report, page 3, second sentence, Contingence Planning: Instead of a complex-wide protective force contingency plan, recommend organizational or site plans. A DOE complex-wide plan is not practical because of different funding sources and protective force contractor organizations.

The Office of Environmental Management (EM) concurs with Recommendations 1, 3, and 4, and has the following comment concerning Recommendation 2. EM is reviewing all of its contracts to ensure that we are setting expectations and driving the performance through the contract. Their stated goal is to safely accelerate risk reduction and cleanup; a key element in achieving this goal is to ensure that our supports costs, which include safeguards and security, do not cost any more than they should. That being said, EM endorses the spirit of the Recommendation, however, is concerned that following the letter of the Recommendation may cause them to measure and monitor the wrong set of performance indicators.

The Office of Energy Efficiency and Renewable Energy had no comments.

Please contact Mark Thornock of my office at 301-903-2995 if you have any questions or comments.

Approved: _____
Under Secretary for Energy, Science and Environment

Disapproved: _____
Under Secretary for Energy, Science and Environment

Date: 4/2/03

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

APR 0 2 2003

MEMORANDUM FOR Fredrick D. Doggett
Deputy Assistant Inspector General
for Audit Services

FROM: Anthony R. Lane
Associate Administrator
for Management and Administration

SUBJECT: Comments on Protective Force Management IG Draft Report

The National Nuclear Security Administration (NNSA) appreciates having had the opportunity to have reviewed the Inspector General's (IG) draft report, "Management of the Department's Protective Forces." We understand that, from previous reports, the IG had noted a number of efficiency-related concerns with the management of its protective forces. In light of those concerns and the change in threat level, the IG initiated this audit to determine whether the Protective Force Program is adequately being managed.

The draft report noted that there have been improvements in the management of the protective forces but the IG believed that there were still a number of challenges that could adversely affect the program. The IG observed:

- long delays associated with granting clearances for newly employed officers
- increases in unscheduled overtime costs
- morale and potential retention problems based on mandatory overtime and declining training opportunities
- operational vulnerabilities associated with unscheduled work stoppages

While the draft report did give credit for having taken a number of actions to reduce the impact of the change in threats, the report makes several recommendations to:

- increase the use of pre screening in conjunction with the Accelerated Access Authorization Program (AAAP) to improve the timeliness of the clearance process
- incorporate performance expectations into the management contracts directed at administering protective force overtime costs

Printed with soy ink on recycled paper

- develop a protective force contingency plan
- Track protective force overtime costs and attrition rates as a means to monitor the effectiveness of workforce management initiatives at the contractor and program level.

While NNSA generally agrees with the draft report and the recommendations, we believe that incorporating performance expectation into the management contracts focused on administering protective force overtime costs would be counterproductive. Overtime is inherent to security operations and also occurs with delays in processing security clearances and with increased demands for security officers. Delays in the clearance process, as you are aware, may be caused by FBI or OPM backlog of clearance investigations, or by clearance adjudication, or by candidates not meeting criteria for AAAP - thereby having to go through the normal or expedited process. While it may be cause for additional review, NNSA's Site Managers will have to determine what is an acceptable level of overtime to be charged to their contracts. This then would differ from site to site depending on specific needs, situations, and risks. I would also like to point out that the NNSA has not granted any waivers regarding firearms requalification, as indicated in the draft report.

The development of a protective force contingency plan, as mentioned in the draft report, is laudable. The difficulties arise, short of rule making, from having multiple unions representing the protective force officers, multiple contractors (NNSA does not have the same protective force contractor throughout their complex), and separate contracts for each site.

Should you have any questions, please contact Richard Speidel, Director, Policy and Internal Controls Management, at 586-5009.

cc: Greg Rudy, Associate Administrator for Facilities and Operations, NA-50
John C. Todd, Chief, Defense Nuclear Security, NA-3.3
Robert Braden, Senior Procurement Executive, NA-63
David Marks, Director, Field Financial Management, Service Center, NV

IG Report No.: DOE/IG-0602

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

5

United States General Accounting Office

GAO

Testimony

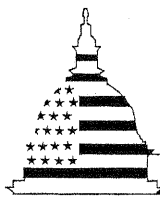
Before the Subcommittee on National Security, Emerging Threats, and International Relations, House Committee on Government Reform

For Release on Delivery
Expected at 9:00 a.m. EDT
June 24, 2003

NUCLEAR SECURITY

DOE Faces Security Challenges in the Post September 11, 2001, Environment

Statement of Robin M. Nazzaro, Director
Natural Resources and Environment Team



G A O

Accountability * Integrity * Reliability

GAO-03-896TNI

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our work for this Subcommittee on physical security at the Department of Energy (DOE) and the National Nuclear Security Administration (NNSA)—a separately organized agency within DOE.[1] DOE and NNSA recognize that a successful terrorist attack on a facility that contains nuclear weapons or nuclear weapons materials could have devastating consequences for the facility and its surrounding communities.

DOE and NNSA rely on their safeguards and security programs to ensure the physical security of NNSA's nuclear weapons complex. Currently, the complex has four production sites—in Missouri, South Carolina, Tennessee and Texas—and three national laboratories that design nuclear weapons in California and New Mexico. DOE's Office of Environmental Management is responsible for cleaning up former nuclear weapons sites that contain some nuclear weapons materials, including sites in Colorado and Washington State. To implement their safeguards and security programs, NNSA and the Office of Environmental Management rely on contractors that are responsible for conducting day-to-day security activities and adhering to DOE policies. The contractors' activities are subject to DOE/NNSA oversight. NNSA and the Office of Environmental Management have offices—site offices—co-located with each site.

Over the past decade, we and others have raised concerns about the adequacy of security at nuclear weapons facilities within the department and NNSA. For example, we reported to you last month that NNSA needs to better manage its safeguards and security program.[2] Concern over security within the nuclear weapons complex was brought into sharper focus by the September 11, 2001, terrorist attacks. These attacks highlighted the importance of effective physical security in response to a challenging and well-organized terrorist threat.

Following the September 11 terrorist attacks, you asked us to review physical security at DOE and NNSA's most sensitive facilities—those

[1]Physical security is the combination of operational and security equipment, personnel, and procedures used to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts.

[2]U.S. General Accounting Office, *Nuclear Security: NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471 (Washington, D.C.: May 30, 2003).

facilities that contain specified quantities of plutonium and highly enriched uranium, which require the Category I level of protection—the highest protection requirement.[3] As agreed with your office, we examined two issues. First, we reviewed how NNSA manages its safeguards and security program. Second, we examined DOE's response to the terrorist attacks of September 11, 2001. In this regard, we examined (1) DOE's and NNSA's immediate response to the attacks; (2) DOE's efforts to develop the design basis threat (DBT), a classified document that identifies the potential size and capabilities of the terrorist forces that DOE and NNSA sites must be prepared to defend against; and (3) the challenges DOE and NNSA face in meeting the requirements of the new DBT.

To carry out our objectives, we reviewed DOE policy and planning documents, including orders, implementation guidance, and reports. We met with officials from DOE and NNSA headquarters and NNSA site offices. We obtained information primarily from DOE's Office of Security, Office of Independent Oversight and Performance Assurance, and Office of Environmental Management; and NNSA's Office of Defense Nuclear Security and NNSA's Nuclear Safeguards and Security Program.[4] We visited NNSA's four production plants and the three design laboratories as well as NNSA's Office of Transportation Safeguards. We also visited four Office of Environmental Management sites that contain Category I special nuclear materials. At each location we met with both federal and contractor officials, observed their physical security operations and obtained and reviewed pertinent supporting documentation, including corrective action plans.

We performed our review from December 2001 through May 2003 in accordance with generally accepted government auditing standards.

[3]Category I special nuclear material that requires Category I level of protection includes plutonium and highly enriched uranium in the form of (1) assembled nuclear weapons and test devices; (2) specified quantities of products containing higher concentrations of plutonium or uranium, such as major nuclear components, and recastable metal; and (3) specified quantities of high-grade materials, such as carbides, oxides, solutions, and nitrates.

[4]We did not include naval reactors in our review because that office is a semiautonomous entity within NNSA with a unique security structure and program.

In summary, we found NNSA has not been fully effective in managing its safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from adversaries seeking to inflict damage. Specifically, we found the following:

- NNSA has not fully defined clear roles and responsibilities for its headquarters and site operations.

- Without a stable and effective management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among NNSA site offices on how they assess contractors' security activities. Consequently, NNSA cannot be assured that all facilities are subject to the comprehensive annual assessments that DOE policy requires.

- To compound the problems in conducting security assessments, NNSA contractors do not consistently conduct required analyses in preparing corrective action plans. As a result, potential opportunities to improve physical security at the sites are not maximized because corrective actions are developed without fully considering the problems' root causes, risks posed, or the cost versus benefit of taking corrective action.

- NNSA has shortfalls at its site offices in the total number of staff and in expertise, which could make it more difficult for site offices to effectively oversee security activities.

We made four recommendations designed to improve NNSA's security management and oversight. NNSA concurred with two of our four recommendations and has made progress in addressing the issues we identified, including publishing a *Safeguards and Security Functions, Responsibilities, and Authorities Manual* and developing and issuing guidance for corrective action plans. Beyond these changes, sustained attention and commitment to sound safeguards and security management will be needed as DOE and NNSA adjust to the post-September 11 security environment.

With respect to DOE's and NNSA's response to the September 11 terrorist attacks, we found that the department has taken a number of important steps to respond to the terrorist threat; however, DOE's response has been slow in some vital respects, and DOE and NNSA will need at least several years and an as yet undetermined amount of resources before their sites

are fully prepared to meet the projected threat. Specifically, we found the following:

- DOE and NNSA took immediate steps to improve security in the aftermath of the September 11 terrorist attacks. For example, DOE and NNSA moved to a higher level of security that required, among other things, more vehicle inspections and security patrols. While these steps are believed to have improved DOE and NNSA's security posture, they have been expensive and, until fully evaluated, their effectiveness is uncertain.

- The number and capabilities of the terrorists involved in September 11 attacks rendered obsolete DOE's DBT, last issued in 1999. However, DOE's effort to develop and issue a new DBT took almost 2 years; it issued the new DBT in May 2003. The effort to develop a new DBT was slowed by, among other things, disagreements over the size of the potential terrorist group that might attack a DOE or NNSA facility.

- Successfully addressing the increased threats contained in the new DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, DOE does not have a reliable estimate of the cost to fully protect DOE and NNSA facilities against the new DBT. DOE and NNSA are developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated. However, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Finally, DOE and NNSA will have to change how they perform physical security through such actions as employing new technologies, consolidating special nuclear materials, and closing unneeded facilities.

Background

From the beginning of the Manhattan Project in the 1940s, a primary mission of DOE and its predecessor organizations has been to design, test, and build the nation's nuclear weapons. To accomplish this mission, DOE constructed a vast nuclear weapons complex throughout the United States. Much of this complex was devoted to the production and fabrication of weapons components made from two special nuclear materials—plutonium and highly enriched uranium.

The end of the Cold War changed the department's focus from building new weapons to extending the lives of existing weapons, disposing of surplus nuclear material, and cleaning up no longer needed weapons sites.

NNSA is responsible for extending the lives of existing weapons in the stockpile and for ultimately disposing of surplus nuclear material, while the Office of Environmental Management is responsible for cleaning up former nuclear weapons sites. Contractors, who are responsible for protecting classified information, nuclear materials, nuclear weapons, and nuclear weapons components, operate both NNSA and Office of Environmental Management sites.[5,6]

Besides NNSA and the Office of Environmental Management, DOE has two other important security organizations. DOE's Office of Security develops and promulgates orders and policies, such as the DBT, to guide DOE and NNSA's safeguards and security programs. DOE's Office of Independent Oversight and Performance Assurance supports DOE and NNSA by, among other things, independently evaluating the effectiveness of contractors' performance in safeguards and security. It also performs follow-up reviews to ensure that contractors have taken effective corrective actions and appropriately addressed weaknesses in safeguards and security.

A key component of DOE's protective strategy is the DBT, a classified document that identifies the characteristics of the potential threats to DOE assets. The DBT considers a variety of threats in addition to terrorists: criminals, psychotics, disgruntled employees, violent activists, insiders, and spies. The terrorist threat is generally the most demanding threat contained in the DBT. The DBT has traditionally been informed and shaped by classified multiagency intelligence assessments of potential terrorists threats. The basis for DOE's 2003 DBT is an intelligence community assessment entitled the *Postulated Threat to U.S. Nuclear Weapons Facilities and other Selected Strategic Facilities* (henceforth referred to as the Postulated Threat).

DOE counters the terrorist threat specified in the DBT with a multifaceted protective system. While specific measures vary from site to site, all protective systems at DOE's and NNSA's most sensitive sites employ a defense-in-depth concept that includes

[5]Responsibility for the Idaho National Environmental Engineering Laboratory has been transferred to DOE's Nuclear Energy Program.

[6]An exception is the Office of Transportation Safeguards, whose protective forces are Special Federal Agents.

- a variety of integrated alarms and sensors capable of detecting intruders;
- physical barriers, such as fences and anti-vehicle obstacles;
- numerous access control points, such as turnstiles, badge readers, vehicle inspection stations, special nuclear material detectors, and metal detectors;
- operational security procedures, such as a "two person" rule that prevents only one person from having access to special nuclear material;
- hardened facilities and/or vaults; and
- a heavily armed paramilitary protective force equipped with such items as automatic weapons, night vision equipment, body armor, and chemical protective gear.

Depending on the material, protective systems at DOE and NNSA Category I sites are designed to accomplish the following objectives in response to the terrorist threat.

- **Denial of access.** For some potential terrorist scenarios, DOE employs a protection strategy that requires the engagement and neutralization of an adversary before the adversary can acquire hands-on access to the assets.
- **Denial of task.** For assets that might present terrorists with opportunities to steal a nuclear weapon or nuclear test device, DOE requires the prevention and/or neutralization of the adversary before the adversary can complete a specific task.
- **Containment with recapture.** In scenarios where the theft of nuclear material (instead of a nuclear weapon) is the likely terrorist objective, DOE requires that adversaries not be allowed to escape the facility and that DOE protective forces recapture the material as soon as possible. This objective requires the use of specially trained and well-equipped special response teams.

The effectiveness of the protective system is formally and regularly examined through a vulnerability assessment. A vulnerability assessment is a systematic evaluation process in which qualitative and quantitative techniques are applied to detect vulnerabilities and arrive at effective protection of specific targets, such as special nuclear material. To conduct this assessment, DOE uses, among other things, subject matter experts, such as U.S. Special Forces; computer modeling to simulate attacks; and

force-on-force performance testing, in which the site's protective forces undergo simulated attacks by an adversary team.

The results of these assessments are documented at each site in a classified document known as the Site Safeguards and Security Plan. In addition to identifying known vulnerabilities and risks and protection strategies for the site, the Site Safeguards and Security Plan formally acknowledges how much risk the contractor and DOE are willing to accept. Specifically, for more than a decade, DOE has employed a risk management approach that seeks to direct resources to its most critical assets—in this case specified quantities of Category I special nuclear material—and mitigate the risks to these assets to an acceptable level. DOE strives to keep its most critical assets at a low risk level and may insist on immediate compensatory measures should a significant vulnerability develop. Compensatory measures could include such things as deploying additional protective forces.

Through a variety of complementary measures, DOE ensures that its safeguards and security policies are being complied with and are performing as intended. Contractors perform regular self-assessments and are encouraged to uncover any problems themselves. In addition to routine oversight, DOE and NNSA site offices are required by DOE Orders to conduct comprehensive annual surveys of contractors' operations for safeguards and security. These surveys, which can draw upon subject matter experts throughout the complex, generally take about 2 weeks to conduct and cover such areas as program management, protection program operations, information security, nuclear materials control and accountability, and personnel security. The survey team assigns ratings of satisfactory, marginal, or unsatisfactory. Currently, most of the DOE and NNSA facilities that we examined have been rated satisfactory in most areas. All deficiencies (findings) identified during a survey require the contractors to take corrective action. DOE's Office of Independent Oversight and Performance Assurance provides yet another check through its comprehensive inspection program. This office performs such inspections roughly every 18 months at each DOE and NNSA site that has Category I special nuclear material.

NNSA Needs to Better Manage Its Safeguards and Security Program

As we reported to you on May 30, 2003, NNSA has not been fully effective in managing its safeguards and security program in four key areas, and therefore it cannot be assured that its contractors are working to maximum advantage to protect critical facilities and materials from individuals seeking to inflict damage. The four key areas are the following:

- **Defining clear roles and responsibilities.** Since its creation in March 2000, NNSA's management structure has been in a state of flux. In December 2002, NNSA issued what it considers final directives for reorganizing headquarters and site offices; however, NNSA expects it will take until at least September 2004 to fully implement its new management structure. This still-developing management structure has led to confusion about the safeguards and security roles and responsibilities of headquarters and site offices. For example, at the time of our review, NNSA headquarters could not provide details on how it intends to (1) monitor the NNSA site offices' performance with respect to safeguards and security or (2) address deficiencies. At the end of May 2003, however, NNSA released a *Safeguards and Security Functions, Responsibilities and Authorities Manual.* This manual, which NNSA itself recognizes as crucial, is intended to set out roles and responsibilities clearly.

- **Assessing sites' security activities.** Without a functional management structure and with ongoing confusion about roles and responsibilities, inconsistencies have emerged among the NNSA sites on how to conduct key aspects of safeguards and security assessment activities. In particular, three out of the seven NNSA site offices use the traditional survey approach, as required by DOE policy, to oversee security activities, while four have discontinued surveys and instead rely on surveillance activities. The distinction between these two activities is important: A survey provides a comprehensive annual review, by a team of experts from throughout NNSA, of contractor safeguards and security and generally takes about 2 weeks. In contrast, surveillance relies on a single or small number of NNSA site officials to oversee one or more aspects of a contractor's safeguards and security activities throughout the year. However, officials from DOE's Office of Security—which developed the policy for conducting surveys—believe the surveillance model does not comply with the DOE order because it does not provide a comprehensive overview. Furthermore, officials from DOE's Office of Independent Oversight and Performance Assurance and NNSA headquarters have expressed concern about the site offices' ability to conduct surveillance because of shortfalls in available expertise. The four site offices have been able to operate using only surveillance activities because, during the reorganization of the management structure, NNSA has not issued guidance on complying with DOE policy for conducting surveys.

- **Overseeing contractors' corrective actions.** NNSA contractors do not consistently conduct the analyses DOE policy requires in preparing corrective action plans, which compounds the problems of ensuring physical security. Inconsistency occurs because the NNSA site officials do not have implementation guidance from headquarters on how to address corrective actions. Of the 43 corrective action plans we reviewed for 1999 through 2002, less than half showed that the contractor had performed the required root cause analysis. Furthermore, less than 25 percent demonstrated that the contractor had performed a required risk assessment or cost-benefit analysis. As a result, potential opportunities to improve physical security at the sites were not maximized because corrective actions were developed without fully considering the problems' root causes, risks posed, or cost versus benefit of taking corrective action. However, at the seven sites we visited in 2002, the site offices and contractors are making some progress in establishing formal processes for root cause and other analyses. Nevertheless, inconsistencies remain regarding the approaches used to complete these analyses. For example, some site processes specify that root cause analyses will be conducted for all corrective action plans, while other sites consider the completion of these analyses optional. NNSA did, however, recently issue guidance to its sites regarding compliance with DOE Orders on corrective actions.

- **Allocating staff.** NNSA has shortfalls at its site offices in the total number of staff and in areas of expertise, which could make it more difficult for the site offices to oversee safeguards and security effectively and to ensure that the agency fully knows security conditions at its sites. According to officials at five of the seven site offices we visited, they have, or expect to have, an average of 2 to 6 vacancies per site for overseeing contractors' safeguards and security; typically, each site expects to have 10 to 14 security-related positions within the next 2 years. The vacancies occur, in part, because staff are reluctant to move to locations they view as less desirable and because NNSA has frozen hiring in response to budget constraints. Some of these vacancies are for specialists in particular subject areas, such as Industrial Security Systems—a key specialty needed for conducting physical security inspections. The lack of expertise and staff could be further complicated for some sites by NNSA's realignment plan. Under this plan, NNSA expects to streamline federal oversight of contractors and reduce headquarters and field staff by 20 percent by the end of fiscal year 2004. Site officials said that they will fill some vacancies through a virtual organization in which experts at other locations will assist with certain components of the surveillance activities. However, it will take time to work through some of the difficulties associated with making the transition to this approach.

DOE and NNSA's Response to the Terrorist Attacks of September 11, 2001

I would like now to discuss DOE and NNSA's response to the terrorist attacks of September 11, 2001. I will cover DOE's and NNSA's immediate response to the attacks; DOE's efforts to develop a new DBT that DOE and NNSA sites must be prepared to defend against; and the challenges DOE and NNSA face in meeting the requirements of the new DBT.

DOE and NNSA Improved Security after September 11, 2001, but Have Not Fully Tested These Improvements

DOE and NNSA took immediate steps to improve physical security in the aftermath of the September 11, 2001, terrorist attacks. These steps included the following:

- **Raised the Level of Security Readiness.** DOE's most visible effort involved moving to higher levels of security readiness, as outlined by DOE Notice 473.6. This notice specifies DOE Security Condition, or SECON, levels and the corresponding security measures that have to be implemented.[7] On September 11, 2001, within a matter of hours, DOE and NNSA sites went from their then-normal SECON level 4—terrorist threat level low—to SECON level 2—terrorist threat level high. Sites were required to implement nearly 30 additional measures, such as increasing vehicle inspections and badge checks; increasing stand-off distances between public and sensitive areas; activating and manning emergency operations centers on a continuous basis; and more heavily arming and increasing the number of protective forces on duty. Sites maintained SECON level 2 through October 2001 before dropping to an enhanced SECON level 3. The sites have returned to SECON level 2 several times since September 11 2001, most recently in May 2003, when the national threat warning systems was elevated to Orange Alert. The new baseline for security at DOE and NNSA facilities is generally assumed to be at an enhanced SECON level 3. This level is still substantially greater than DOE's pre-September 11, 2001 security posture.

- **Enhanced Protective Force Responses.** On October 3, 2001, the Secretary of Energy issued a classified directive that ordered more robust protective force responses and increased levels of performance testing for the protection of certain special nuclear material at DOE's and NNSA's most critical facilities.

[7]SECON levels are pegged to the national threat level issued by the Department of Homeland Security. For example, a national level of ORANGE equates to SECON level 2 for DOE facilities.

- **Conducted Security Reviews, Studies and Analyses.** DOE and NNSA also conducted a number of security-related reviews, studies, and analyses. For example, within days after the terrorist attacks, DOE and NNSA officials conducted a classified assessment of their facilities' vulnerabilities to an attack such as the one on September 11. This assessment came to be known as the *72 Hour Review*. In addition, NNSA organized a 90-day Combating Terrorism Task Force, composed of 12 federal and contractor employee teams that looked at a number of security areas. One team, the site-by-site security review and vulnerability assessment group, identified over 80 prioritized security improvement projects, totaling more than $2 billion, that could be completed within 5 to 6 years. These projects ranged from hiring additional protective forces to consolidating special nuclear material.

- **Increased Liaison with Federal, State, and Local Authorities:** Before the September 11 terrorist attacks, DOE and NNSA headquarters offices and sites maintained a variety of relationships, memoranda of understanding, and other formal and informal communications with organizations such as the Federal Aviation Administration, Federal Bureau of Investigation, and state and local law enforcement and emergency management agencies. After the terrorist attacks, DOE and NNSA officials increased their communication with these organizations and established direct links through sites' emergency operations centers. Because of the potential threat of aircraft attacks created by the September 11 attacks, sites worked closely with the Federal Aviation Administration and the U.S. military.

While these steps are believed to have generally improved security, they have been expensive and, until fully tested using DOE's vulnerability analysis approach, their effectiveness is uncertain. With respect to improved security, implementation of SECON levels 2 and 3 has, for example, increased the visible deterrence at DOE and NNSA sites by placing more guards around the sites. Studies and analyses, such as the *72 Hour Review*, have also resulted in different and less vulnerable storage strategies for some special nuclear material. DOE and NNSA have hired additional protective forces and are training them. Finally, some long-recognized security enhancement projects have received more funding, such as the construction of a new highly enriched uranium materials facility at the Y-12 Plant, and the removal of some of the Los Alamos National Laboratory's most sensitive materials and equipment to a more modern facility at the Nevada Test Site have been accelerated.

At the same time, it has been expensive to implement the increased SECON measures. DOE and NNSA sites estimate that it costs each site

from $18,000 to nearly $200,000 per week in unplanned expenditures to implement the required SECON level 2 and 3 measures. Most of these expenses result from overtime pay to protective forces.

However, the costs of the higher SECON levels can be measured in more than just budget dollars. For example, a recent DOE Inspector's General report found that the large amounts of overtime needed to meet the higher SECON requirements have resulted in fatigue, reduced readiness, retention problems, reduced training, and fewer force-on-force performance tests for the protective forces.[8] In addition, the increased operational costs associated with the higher SECON levels can hinder or preclude sites from making investments that could improve their security over the long term. For example, one site delayed purchasing equipment for its protective force that would address a known vulnerability because of the high costs of SECON implementation. Finally, implementation of the protective force response plans outlined in the Secretary's October 3, 2001, directive was sharply limited by the lack of available funding, with some sites estimating it would take from about $30 million to over $200 million to implement the directive completely. Moreover, the performance testing requirements of this directive were generally not conducted because of the already large amounts of protective force overtime required by the higher SECON levels. The new DBT, however, has replaced this directive.

Other than deterrence, the role of the higher SECON levels in improving DOE and NNSA physical security is uncertain. Some aspects of the SECON measures, such as vehicle inspection checkpoints have undergone some limited testing of their effectiveness. However, the higher SECON level measures in place at most sites have not been assessed using the vulnerability assessment tools, such as computer modeling and full-scale force-on-force exercises, that play such a key role in developing protective strategies for DOE and NNSA sites.

Finally, while liaison with other agencies is important, DOE and NNSA site officials anticipate that terrorist attacks on their facilities will be short and violent affairs and will be over before any external responders can arrive on site. In addition, because some DOE and NNSA sites are close to airports and/or major flight routes, they may receive little warning of

[8] *Audit Report: Management of the Department's Protective Forces*, DOE/IG-0602, Department of Energy Office of the Inspector General, June 2003.

aircraft attacks and U.S. military aircraft may have little opportunity to intercept these attacks.

Development of a New DBT Was Difficult, but Resulted in a Higher Threat Level

In the immediate aftermath of September 11, 2001, DOE and NNSA officials realized that the then current DBT, issued in 1999 and based on a 1998 intelligence community assessment, was largely obsolete. The terrorist attacks suggested larger groups of adversaries, larger vehicle bombs, and broader terrorist aspirations to cause mass casualties and panic than were envisioned in the 1999 DOE DBT. However, formally recognizing these new threats by updating the DBT has proven difficult.

The traditional basis for the DBT has been a study, known as the Postulated Threat, conducted by the U.S. intelligence community and agency security organizations, principally the Department of Defense's (DOD) Defense Intelligence Agency. However, the new Postulated Threat was completed about 9 months behind its original schedule and not finally released until January 2003. According to DOE and DOD officials, this delay was the result of other post-September 11, 2001, demands placed on the intelligence community as well as sharp debates among the organizations involved with developing the Postulated Threat over the size and capabilities of future terrorist threats and the resources needed to meet these projected threats.

Given the delay associated with the development of the Postulated Threat, DOE, on its own, developed a number of draft threat statements that culminated in the final May 20, 2003, DBT. These included the following:

- **December 2001—Interim Joint Threat Policy Statement.** DOE and DOD worked on this joint draft document but abandoned this effort later in 2002.
- **January 2002—Interim Implementing Guidance.** DOE's Security Office issued this guidance so that DOE and NNSA programs could begin to plan for eventual increases in the DBT.
- **May 2002—Draft DBT.** DOE produced its official draft DBT. This was labeled an interim product pending the release of the Postulated Threat.
- **August 2002—2nd Draft DBT.**
- **December 2002—3rd Draft DBT.**

- **April 2003—4th Draft DBT.**

- **May 2003—Final DBT.**

DOE's Security Office distributed the drafts to DOE and NNSA program and site offices and invited them to provide comments. DOE's Security Office considered these comments and often incorporated them into the next version of the DBT. DOE's Security Office also continued to coordinate with the other federal organizations that have similar assets, chiefly DOD and the Nuclear Regulatory Commission.

During the development of DOE's DBT, debates, similar to those that occurred during the development of the Postulated Threat, emerged in DOE and NNSA over the size of the future threat and how much it would cost to meet the new threat. DOE and NNSA officials from all levels told us that concern over resources played a large role in developing the 2003 DBT, with some officials calling the DBT the "funding basis threat," or the maximum threat the department could afford. This tension between threat size and resources is not a new development. According to a DOE analysis of the development of prior DBTs, political and budgetary pressures and the apparent desire to reduce protective force manpower requirements appear to have played a significant role in determining the adversary numbers contained in prior DBTs.

Reflecting the post-September 11, 2001, environment, the 2003 DBT is a substantially different and more demanding document than previous DBTs. Key differences from the 1999 DBT include the following:

- **Increased adversary threat levels.** The 2003 DBT increases the terrorist threat levels for the theft of the department's highest value assets—special nuclear material—although not in a uniform way. The 1999 DBT required DOE and NNSA sites to protect against only one terrorist threat level. Under the 2003 DBT, however, the theft of a nuclear weapon or test assembly is judged to be more attractive to terrorists, and sites that have these assets are required to defend against a substantially higher number of adversaries than are other DOE and NNSA sites that possess other forms of Category I quantities of special nuclear material. For example, the Pantex Plant, which, among other things, assembles and disassembles nuclear weapons, is required to defend to a higher level than sites such Los Alamos or Y-12, both of which fabricate nuclear weapons components. DOE calls this a graded threat approach.

- **Specific protection strategies.** In line with the graded threat approach and depending on the type of materials they possess and the likely mission of the terrorist group, sites are now required to implement specific protection strategies, such as denial of access, denial of task, or containment with recapture for their most sensitive facilities and assets.

- **Wider range of terrorist objectives.** The 2003 DBT recognizes a wider range of terrorist objectives, particularly in the area of radiological, chemical, and biological sabotage. The 2003 DBT requires the development of protection strategies for a range of facilities, such as some radioactive waste storage areas, that were not covered under the previous DBT.

- **Increased Complexity.** With a graded approach and broader coverage, the new DBT is a more complex document than its predecessor. For example, the 1999 DBT was 9 pages long, while the 2003 DBT is 48 pages long.

During the 21 months it took to develop the DBT policy, DOE and NNSA sites still officially followed the 1999 DBT, although their protective posture was augmented by implementing SECON level 2 and 3 measures. While DOE sites under the Office of Environmental Management continued to conduct vulnerability assessments and develop Site Safeguards and Security Plans based on the 1999 DBT, NNSA largely suspended the development of Site Safeguards and Security Plans pending the issuance of the new DBT. During this period, however, NNSA did embark on a new vulnerability assessment process, called Iterative Site Analysis, at four sites and its Office of Transportation Safeguards. The Iterative Site Analyses were analytical, tabletop exercises that addressed a spectrum of potential threats, both within and beyond the threat contained in the 1999 DBT. Iterative Site Analyses were conducted by independent and highly skilled security professionals from across the government and private sector. Most NNSA sites agreed that the Iterative Site Analysis exercises were valuable, and some sites believe that it gave them a head start in meeting the requirements of the new DBT. The Office of Environmental Management is testing this methodology at one of its sites this summer. DOE's Office of Independent Oversight and Performance Assurance continued its inspections; however, it initially reduced the amount of force-on-force performance testing it conducted because of the high levels of protective force overtime caused by implementation of SECON level 2 and 3 measures. This Office also planned to begin performance testing at levels beyond the 1999 DBT, but had done so at only one site before the 2003 DBT was issued.

Implementation of the 2003 DBT Will Be Challenging

Successfully addressing the increased threats contained in the 2003 DBT will take time and resources, as well as new ways of doing business, sound management, and leadership. Currently, the department does not have a reliable estimate for the total cost of fully protecting DOE and NNSA facilities against the 2003 DBT. While DOE and NNSA officials expect new resource requirements to vary widely among the sites, neither the current fiscal year 2003 nor the planned fiscal year 2004 budget includes funds for implementing the 2003 DBT. DOE and NNSA are currently developing preliminary cost estimates that could be included in the fiscal year 2005 budget, which is now being formulated; however, the fiscal year 2006 budget will probably be the first to show the full budgetary impact of the new DBT. DOE and NNSA officials suggest that in order to take earlier action, they may pursue additional security funding through reprogramming and/or supplemental appropriations.

Once funds become available, most sites estimate that it will take from 2 to 5 years to fully implement, test, validate, and refine strategies for meeting the new DBT requirements. Some sites, particularly those that benefited from the Iterative Site Analysis, may be able to move more quickly, and all sites will continue to place priority on improving the protection of special nuclear material.

DOE and NNSA officials also recognize that they will have to change how they perform the physical security mission. A DOE 1999 report and a 2002 NNSA report, this time reinforced by the September 11 attacks, called for changes in the way the department approaches physical security.[9] These changes will be even more important now that the 2003 DBT has been issued. DOE and NNSA are seeking to

- develop and employ new technologies;
- accelerate the design and construction of new facilities;
- better utilize existing facilities;
- purchase adjacent public lands, close public roads and/or build bypass roads around key facilities to restrict public access; and

[9] *A Context and Strategy for Action: A Synthesis of the Special Security Review for DOE Executive Management*, December 1998; *A Security Architecture for NNSA: A Proposed Framework for Planning and Managing Security*, May 23, 2002.

- consolidate special nuclear material and close unneeded facilities.

DOE and NNSA have taken some steps in these directions, but will have to accomplish more to meet the post-September 11, 2001, security challenges. For example:

- **Developing and Employing New Technologies.** Security at many DOE and NNSA sites is a manpower-intensive activity. Adding additional protective forces to facilities is a flexible, effective, but ultimately expensive way of providing additional security. DOE's Security Office has funded a technology development and assessment program and NNSA is initiating its own program in fiscal year 2004; however, the amount of funds devoted to these activities has been limited. The use of technology in areas such as communications, weaponry, intrusion detection, and better computer modeling offers the promise of more effective security at, ultimately, lower costs.

- **Accelerating the Design and Construction of New and Better Protected Facilities.** It is difficult, expensive, and sometimes impossible to retrofit existing facilities to meet more demanding physical security requirements, such as those identified in the 2003 DBT. It is far better to make security an integral part of the design of a new facility. For example, DOE estimated that a new facility built to centrally store special nuclear material would have very steep up-front costs of $2.5 to $4 billion, but would pay for itself in 4 years because of savings from reducing the number protective forces and reducing costs for safeguards and security maintenance. While DOE is not currently planning for such a facility, it is now designing or constructing a number of new facilities at several sites that will be better protected than existing facilities, although their level of protection against the 2003 DBT is uncertain. One of these new facilities, the highly enriched uranium materials facility at the Y-12 plant, may be completed as early as fiscal year 2008.

- **Better Utilization of Existing Facilities.** DOE and NNSA had made some progress in this area, even before September 11, 2001. For example, the old K Area Reactor at the Savannah River Site, a massively constructed building already outfitted with physical security systems, was converted to an interim plutonium storage facility and is currently accepting shipments of plutonium from Rocky Flats. In addition, planning is underway to move sensitive equipment and materials from Technical Area –18 at Los Alamos to the more modern Device Assembly Facility at the Nevada Test Site. However, this move is expected to cost $130 million and not be completed until fiscal year 2009.

- **Purchasing Adjacent Public Lands, Closing Public Roads and/or Building Bypass Roads Around Key Facilities to Restrict Public Access.** A number of sites are bisected or adjacent to public roads and areas. Public access to these roads and areas has been restricted since September 11, 2001, and more permanent measures are being implemented or studied at sites such as Pantex, Lawrence Livermore, Los Alamos, and Y-12.

- **Closing Unneeded Facilities and Consolidating Special Nuclear Material.** DOE's Office of Environmental Management has long had the goal of closing unneeded facilities and consolidating special nuclear material. The Office of Environmental Management has recently proposed accelerating the deadline from 2016 to 2006 for moving Category I special nuclear material from Hanford and Rocky Flats to its Savannah River Site. At Savannah River, materials will ultimately be disposed of or transferred to other program offices, such as NNSA and DOE's Nuclear Energy Program. The Office of Environmental Management expects that all Category I special nuclear material will be removed from Rocky Flats by the end of the summer, 2003.

In closing, it will be a challenge for DOE and NNSA to deal with the post-September 11 security threats. DOE and NNSA have been providing physical security for over 50 years; however, given the materials and assets they possess, physical security at DOE and NNSA facilities cannot afford to fail, even once.

Meeting these challenges will require DOE and NNSA to provide sustained, sound management for their safeguards and security programs. This is particularly true for NNSA because it is the enduring steward for the nation's special nuclear material and is responsible for ensuring that the nation's nuclear weapons are safe and reliable.

Equally important DOE and NNSA must exercise strong, sustained, and high-level leadership in providing for safeguards and security. Security officials often told us that the department has a history of alternating periods of inattention and attention to security. In the post September 11, 2001, environment, the stakes are too high to allow such lapses in the future.

Mr. Chairman, this concludes my testimony. I would be happy to respond to any questions you or Members of the Subcommittee may have.

GAO Contact and Staff Acknowledgments

For further information on this testimony, please contact Robin M. Nazzaro at (202) 512-3841. James Noel, Jonathan Gill, Chris Pacheco, Andrea Miller, Chris Abraham, and Jill Berman also made key contributions to this testimony.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:

Voice:	(202) 512-6000
TDD:	(202) 512-2537
Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

6

Richard J. Levernier
P.O. Box 146
Germantown, MD 20875

February 10, 2004

Catherine A. McMullen, Esq.
Chief, Whistleblower Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, NW
Washington, DC 20036

Dear Ms. McMullen:

The purpose of this letter is to provide additional comments on the U.S. Department of Energy (DOE) report concerning my whistleblower disclosure. On January 15, 2002, I submitted a whistleblower disclosure to the U.S. Office of Special Counsel (OSC) (File No. DI-02-0572). On October 25, 2002, the OSC determined that there was a "substantial likelihood" that the information contained in my disclosure constituted a substantial and specific danger to public health and safety arising out of actions taken or not taken by officials at DOE concerning physical security at DOE's nuclear weapons facilities. Therefore, OSC transmitted the allegations to the Secretary of Energy for an investigation and report pursuant to 5 USC 1213 (c). Pursuant to the statute, the Secretary had 60 days to conduct an investigation of these allegations and report back to OSC.

Finally, on May 29, 2003, the Secretary of Energy submitted the required report of investigation to OSC. On December 2, 2003, I was contacted by OSC, through my legal counsel, and informed that the DOE report (25 pages in length) was available for my review and comment. On December 19, 2003, I submitted my initial comments on the DOE report concerning my whistleblower disclosure to OSC.

Subsequent to submittal of my comments, on January 23, 2004, the DOE Office of the Inspector General (OIG) issued an Inspection Report entitled, "Protective Force Performance Test Improprieties" (copy attached) which is directly relevant to my whistleblower disclosure since cheating on protective force performance tests was one of the central issues referred by OSC to DOE for investigation. On February 2, 2004, I requested that OSC allow me time to analyze the OIG report and provide additional comments on the DOE investigation of my whistleblower disclosure.

My whistleblower disclosure to OSC stated:

"DOE performance test scenarios are frequently compromised resulting in wholly invalid test results and similarly flawed conclusions concerning protection effectiveness".

"On numerous occasions, DOE performance tests have been compromised, in some cases due to outright and documented cheating."

"DOE could enhance the integrity of its performance testing program, with corresponding benefit to security programs, by developing standard performance test protocols and ethics. DOE policy should also require that all reports of suspected performance test compromises or improprieties be vigorously investigated and appropriately documented. Disciplinary action should be initiated against violators, consistent with the national security implications associated with invalid performance tests."

"There is no DOE standard for MILES equipment. On numerous occasions during actual DOE performance tests the adversaries have been assigned MILES weapons with less than 50% of the weapon's effective range. For example, adversaries have been assigned MILES M-60 machine guns with an effective range of only 200 meters when the actual effective range exceeds 600 meters. At one site, a local DOE official stated the adversary, "must be unfamiliar with the weapon." In reality, the adversary was an active member of US Army Special Forces and had been recently recognized as the US Army's M-60 machine gun champion. The significance of this situation was that an active duty U.S. Army expert machine gunners' performance was seriously degraded because of the limitations of DOE's obsolete and poorly maintained MILES equipment. The tactical disadvantage of this situation for the adversary was very significant and had a corresponding direct negative impact on the validity of the test."

"The performance tests conducted by DOE as a critical element of the comprehensive oversight program and for validation of vulnerability assessments provide flawed results because they are artificial and unrealistic; utilize obsolete or poorly maintained MILES equipment; are evaluated by persons lacking qualifications; are simplistic and clearly not representative of the worst case terrorist threat; and, are frequently compromised due to "cheating" without repercussions."

The DOE OIG Inspection Report, "Protective Force Performance Test Improprieties" states:

"Our inspection confirmed that the results of the June 26, 2003, performance test may have been compromised. We found that shortly before the test, two protective force personnel were inappropriately permitted to view the computer simulations of the four scenarios. This action compromised controlled (test-sensitive) information. As a consequence, the test results were, in our judgment, tainted and unreliable."

During the Office of Inspector General review, several current and former protective force personnel provided us with **compelling testimony that there**

has been a pattern of actions by site security personnel going back to the mid-1980's that may have negatively affected the reliability of site performance testing. We were told, for example, that controlled information had been shared with protective force personnel prior to their participation in a given performance test. This included such important data as: the specific building and wall to be attacked by the adversary; the specific target of the adversary; and, whether or not a diversionary tactic would be employed by the test adversary."

The DOE report of investigation concerning my whistleblower disclosure incorrectly concluded that all of my allegations were unfounded. The DOE OIG Report cited above provides incontrovertible documentary evidence that cheating on protective force performance tests (a central issue in my whistleblower disclosure) has existed at the Y-12 National Security Complex (a major DOE nuclear weapons facility) since the mid-1980s. As stated in my disclosure, cheating on protective force performance tests is a pervasive problem DOE-wide. The DOE's response to this critical issue in my whistleblower disclosure is obviously inadequate since the DOE OIG investigation determined a pattern of cheating has existed since the mid-1980's! This compelling evidence demonstrates that the DOE investigation of the issues contained in my whistleblower disclosure, and referred by OSC after a "substantial likelihood determination", was incomplete and that the report signed by the Secretary of Energy was false.

The U.S. Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 28 January 2004 (copy attached) stated:

"Security guards at the country's leading nuclear storehouse have been cheating during anti-terrorism drills, according to a report released Monday, January 26, by the Department of Energy's inspector general. Now, watchdogs in Congress and beyond are questioning whether the tons of enriched uranium ay the Y-12 National Security Complex in Oak Ridge , TN are really safe at all. Y-12 is America's main facility for processing enriched uranium. It stores nearly all of the country's reserve of about 5000 "secondaries," the thermonuclear hearts of hydrogen bombs."

The DHS analysis cited above questions whether the enriched uranium at Y-12 is really safe at all. The level of security afforded special nuclear material at Y-12 and other DOE facilities is questionable when the protective force performance tests used to validate the effectiveness of protection have been compromised due to outright documented cheating. The OSC should immediately reject the DOE investigation of my whistleblower disclosure as insufficient and incomplete.

In conclusion, I continue to believe that the scope and magnitude of security problems at DOE, which were identified in my whistleblower disclosure more than 2 years ago, constitute a substantial and specific danger to public health and safety. Given the significant increases in the terrorist threat which has been universally acknowledged

since 9/11, the degradation of national security that results from these deficiencies is even greater now. I believe that any objective journeyman nuclear security professional evaluating my whistleblower disclosure, the DOE investigative report concerning my whistleblower disclosure and subsequent directly relevant U.S. General Accounting Office (GAO) and DOE OIG reports and testimony will find the DOE report seriously lacking in credibility. I also believe the new information contained in the GAO testimony referenced in my December 19, 2003, comment letter to OSC, i.e. that DOE will likely not have the financial resources necessary to address the May 2003 DBT until fiscal year 2006, and that it will take an additional 2 to 5 years to implement the required additional security measures, creates an extended window of vulnerability and exacerbates an already unsatisfactory situation. Given that DOE is protecting nuclear weapons and special nuclear materials and recognizing the catastrophic consequences associated with a security breach, only the highest level of protection is acceptable. Uncertainty about DOE's ability to protect nuclear weapons and special nuclear material is unacceptable. Until DOE abandons its longstanding approach of denial for any alleged security problems, our nation will continue to be vulnerable to preventable terrorist threats.

DOE's denial mentality for security deficiencies is clearly apparent with respect to cheating on performance tests. I identified systemic cheating on protective force performance tests at DOE nuclear weapons facilities in my whistleblower disclosure. The DOE investigation of my whistleblower disclosure determined that all of my allegations were unfounded and the Secretary of Energy signed a letter containing that false conclusion to the Special Counsel. Shortly thereafter the DOE OIG issued a formal Inspection Report concluding there has been a pattern of cheating on protective force performance tests going back to the mid-1980's. The protection of national security assets, including special nuclear (weapons) material, in the custody and control of the DOE is not a game. The loss of nuclear weapons or components would have catastrophic consequences and clearly constitutes a substantial and specific risk to public health and safety. Unless OSC takes immediate action on this matter, this significant national security vulnerability will continue unabated and ripe for terrorist exploitation.

I appreciate the opportunity to provide additional comments to OSC on this matter. Please contact me at (301) 903-2178 if you have any questions.

Sincerely,

Original Signed by Richard J. Levernier

Richard J. Levernier

Attachments (2)

7

U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Protective Force Performance Test Improprieties

DOE/IG-0636

January 2004

Department of Energy
Washington, DC 20585

January 23, 2004

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Protective Force Performance Test Improprieties"

BACKGROUND

On June 26, 2003, a protective force performance test was conducted at the Department of Energy's Y-12 National Security Complex, which is a component of the National Nuclear Security Administration (NNSA). The purpose of the test was to obtain realistic data for developing the Y-12 Site Safeguards and Security Plan. The mission at the site includes a number of sensitive activities, such as enriched uranium material warehousing, and weapon dismantlement and storage. These activities necessitate that the site have a protective force capable of responding to potential security incidents such as a terrorist attack.

Computer simulations conducted prior to the June 2003 performance test had predicted that the responder (defending) protective forces would decisively lose two of the four scenarios that comprised the test. When the responder protective forces won all four of the scenarios, the Y-12 Site Manager became concerned that the test may have been compromised. The Manager initiated an inquiry, which identified issues regarding responder protective force personnel having had access to the computer simulations of the four scenarios prior to the performance test. Subsequently, at the Y-12 Site Manager's request, the Office of Inspector General initiated a review to address these issues.

Based on information developed during the course of the review, the scope of the inspection was expanded to examine whether there had been a pattern over time of site security personnel compromising protective force performance tests.

RESULTS OF INSPECTION

Our inspection confirmed that the results of the June 26, 2003, performance test may have been compromised. We found that shortly before the test, two protective force personnel were inappropriately permitted to view the computer simulations of the four scenarios. This action compromised controlled (test-sensitive) information. As a consequence, the test results were, in our judgment, tainted and unreliable.

During the Office of Inspector General review, several current and former protective force personnel provided us with compelling testimony that there has been a pattern of actions by site

Printed with soy ink on recycled paper

security personnel going back to the mid-1980's that may have negatively affected the reliability of site performance testing. We were told, for example, that controlled information had been shared with protective force personnel prior to their participation in a given performance test. This included such important data as:

- The specific building and wall to be attacked by the test adversary;
- The specific target of the test adversary; and
- Whether or not a diversionary tactic would be employed by the test adversary.

Two other protective force contractor employees who were identified as having some level of involvement in these actions denied any such involvement. However, it was clear that if controlled information was, in fact, disclosed prior to the performance tests, the reliability of the information used to evaluate the efficacy of the protective force at the Oak Ridge complex was in question.

The report includes several recommendations to Department management designed to enhance the integrity of future performance tests.

MANAGEMENT REACTION

NNSA concurred with our findings and recommendations and provided a series of corrective actions that either had been initiated or were planned as a result of direction from the NNSA Administrator and the Y-12 Site Office Manager. NNSA's comments, which are provided in their entirety in an appendix to this report, also represent the position of the Oak Ridge Operations Office. The Office of Independent Oversight and Performance Assurance, whose comments are also appended to this report, concurred with our recommendation to that Office.

We found management's comments to be responsive to our recommendations.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Director, Office of Security and Safety Performance Assurance
Director, Office of Science
Manager, Y-12 Site Office
Manager, Oak Ridge Operations Office
Director, Policy and Internal Controls Management

PROTECTIVE FORCE PERFORMANCE TEST IMPROPRIETIES

TABLE OF CONTENTS

OVERVIEW

Introduction and Objectives 1

Observations and Conclusions 3

DETAILS OF FINDINGS

June 26, 2003, Performance Test 4

Performance Testing 5

Performance Measurement 8

RECOMMENDATIONS 9

MANAGEMENT COMMENTS 9

INSPECTOR COMMENTS 9

APPENDICES

A. Scope and Methodology 10

B. Management Comments 11

Overview

INTRODUCTION AND OBJECTIVES

The Department of Energy's (DOE's) Y-12 National Security Complex in Oak Ridge, Tennessee, which is a component of the National Nuclear Security Administration (NNSA), is an integral part of the nuclear weapons complex. The Y-12 mission includes the production of hardware to support nuclear weapon stockpile certification; the precision manufacturing of unique nuclear weapons components; weapon dismantlement, storage, and evaluation; and enriched uranium material warehousing and management, including overseeing the secure management and storage of special nuclear materials. These activities necessitate that the site have a protective force capable of responding to potential incidents such as a terrorist attack.

As part of the security planning process, Department sites identify potential threats and develop plans for addressing them, including protective force response. One of the key tools in this process is protective force performance testing, which is used to determine that the security features of a system are implemented as designed and are adequate for the proposed environment. Protective force performance testing commonly involves live exercises where "responder" protective forces defend against a simulated attack. Performance tests are frequently referred to as force-on-force exercises; however, technically, these constitute just one type of performance test.

Because of the high cost of live protective force performance tests, which at Y-12 we were told cost between $50,000 to $85,000 per test, sites use a computer program to simulate protective force responses to various threats. Select simulations are then validated through performance tests. It is DOE policy that performance tests must be used to, among other things, realistically evaluate and verify the effectiveness of protective force programs, identify and provide needed training, and validate implemented improvements.

On June 26, 2003, a type of Limited Scope Performance Test, locally identified as a Diagnostic Evaluation Exercise, was conducted at Y-12 to obtain realistic data for developing the Site Safeguards and Security Plan. Computer simulations had predicted that the responder protective forces (those defending the site) would decisively lose two of the four scenarios that comprised the performance test. When the responder protective forces won all four of the scenarios, the Y-12 Site Manager became suspicious that the test may have been compromised. The Manager initiated

an inquiry, and concerns surfaced regarding (1) responder protective force personnel having had access to the computer simulations of the four scenarios prior to the performance test and (2) conflicting information over who authorized that access. Subsequently, the Y-12 Site Manager requested assistance from the Office of Inspector General (OIG) to address these concerns.

During our inspection, we were provided information that inappropriate actions had occurred going back to the mid-1980's in connection with performance tests at the Department's Oak Ridge complex. Several different contractors have held the protective force contract during the period in question. These contractors have provided security throughout the Oak Ridge complex, which includes Y-12, the Oak Ridge National Laboratory, the East Tennessee Technology Park, and other Department facilities.

Based upon this information, we expanded our inspection to examine whether there had been a pattern over time of site security personnel compromising protective force performance tests. Also, pursuant to the Government Performance and Results Act of 1993 (GPRA), we reviewed relevant performance measurement processes applicable to the current Oak Ridge complex security contractor, Wackenhut Services, Inc. Wackenhut was awarded the security contract in September 1999 and began operations in January 2000.

OBSERVATIONS AND CONCLUSIONS

Our inspection confirmed the concerns of the Y-12 Site Manager regarding the performance test conducted on June 26, 2003. We found that shortly before the test, two participating protective force personnel were permitted to view the computer simulations of the four scenarios. We concluded that this action was improper, since it had the potential to adversely impact the realism of the performance test and its outcome. In short, the test results were tainted and should not, in our judgment, be relied upon.

During the inspection, we interviewed over 30 current and former site security police officers (SPOs) and SPO supervisors. We received testimony from several individuals that there has been a pattern of actions by site security personnel over an extended period of time that may have negatively affected the realism and, therefore, the reliability of numerous performance tests at the Oak Ridge complex. Several individuals told us, for example, that controlled (test-sensitive) information was shared with SPOs prior to their participation in a given performance test. These concerns paralleled our findings regarding the June 2003 performance test. When queried as to the nature of the information that had been shared with SPOs in prior years, they provided a number of examples, including the following:

- The specific building and wall to be attacked by the test adversary;
- The specific target of the test adversary; and
- Whether or not a diversionary tactic would be employed by the test adversary.

These concerns were expressed by current and former protective force personnel who were in a position to be aware of the facts and circumstances of the prior performance tests. We found their assertions to be credible and compelling. Two protective force contractor employees who were identified as having involvement in these actions denied such activities. We could not find documentary evidence to support or refute the testimonial evidence. However, it was clear that if controlled information was, in fact, disclosed prior to the performance tests, such action would have influenced the reliability of the information used to evaluate the efficacy of the protective force program at the Oak Ridge complex.

JUNE 26, 2003, PERFORMANCE TEST

The Y-12 Site Office Manager raised concerns with respect to the performance test conducted on June 26, 2003. We found that two protective force personnel who were to participate as responders in the test were provided information that could have had a direct bearing on the exercise outcome. Specifically, the day before the performance test, the two individuals were allowed to view computer simulations on the Joint Conflict and Tactical Simulation (JCATS) computer program of the four scenarios that would comprise the performance test. (Because of Privacy Act considerations, specific details regarding the events surrounding their viewing of the scenarios have been provided to the Y-12 Site Office Manager under separate cover.) The two individuals denied that the information to which they were given access affected their actions or directions to others who participated in the exercise. However, when we viewed the computer simulations, it became clear that the occurrence of certain specific events would identify which scenario was being initiated by the aggressor force. The order in which the targets would be attacked was controlled information.

We asked senior Department and contractor personnel if they believed it was appropriate for the two protective force personnel to view the JCATS simulations prior to the exercise. The Y-12 Site Manager said he was aware that members of the protective force participate in computer simulations and have been doing so for several years; however, when the same computer scenarios that will comprise the performance test are viewed by protective force members the day before the exercise, he believed there is a "problem." A senior official for BWXT Y-12, LLC, the site operating contractor, said that by viewing the JCATS scenarios, the protective force personnel gained such an advantage that it raised concerns about the realism of the exercise results. A senior official for Wackenhut at Oak Ridge said that if Wackenhut supervisors inappropriately received information that other responders did not receive, then there was a possibility that a mishandling of information had occurred.

We also consulted with officials outside of Oak Ridge to obtain a broader perspective on this incident. A JCATS expert at Sandia National Laboratories told us that viewing the JCATS simulations prior to an exercise would give away too much information. Similar views were expressed by officials with DOE's Office of Security and an official in NNSA's Office of Defense Nuclear Security.

Based upon the facts and circumstances of this matter, we concluded that it was inappropriate for the two Wackenhut protective force personnel to have been allowed to view the four JCATS scenarios shortly before the performance test. This action had the potential to impact the realism and, therefore, the reliability of the performance test.

PERFORMANCE TESTING

We were provided testimonial information by several current and former protective force personnel that prior to performance tests, including those conducted during DOE Headquarters oversight reviews, controlled information regarding the performance test and specific adversary actions was provided to contractor protective force personnel by contractor management. We were told that this practice spanned from the mid-1980's to the present. Several individuals advised us that the types of information shared included identification of the specific building and wall that would be attacked, the target, and whether a diversionary tactic would be employed prior to initiation of the primary test assault.

While we treated this information as credible based on the job status and responsibilities of those providing the data, we could not find any documentary evidence to support the assertions. The individuals themselves acknowledged that they were not aware of any documentary evidence of these actions.

We were also told by a number of individuals that protective force members had disabled their Multiple Integrated Laser Engagement System (MILES) gear, thus providing the responder force with an unfair advantage. MILES gear is used to determine whether the exercise participant wearing it has received a simulated fatal gunshot and can no longer participate in the exercise. We were told that exercise participants had, at various times in the past, removed the batteries from the MILES gear; put the batteries in backwards; and/or placed material such as tape, mud, or Vaseline over the system sensors, so they would not operate properly.

We learned that new MILES gear purchased at Oak Ridge in 2000 could help to minimize the occurrence of such actions; however, the site is still working on fully implementing its capabilities. For example, although the new gear creates computer-generated information that can be used to reconstruct the activities of each participant to identify if certain types of tampering occurred, such reconstruction did not occur for the two tests we reviewed. Even after full implementation, some avenues for possible abuse will

still exist. For example, the sensors can still be obstructed by an individual applying a material such as tape, mud, or Vaseline.

Current or former protective force personnel provided a number of examples of improper actions related to prior performance tests:

- A protective force responder would be assigned to "tail" the aggressors and observe their movements while they were touring Y-12 buildings and targets prior to and in preparation for an exercise.

- Based on specific attack information, trucks or other obstacles would be staged at advantageous points to be used as barricades and concealment by protective force responders for shooting during the exercises.

- Training prior to a performance test would focus on the specific building to be targeted, and in some instances, an oral plan would be created that deviated from the established Y-12 tactical plan to counter the attack.

- Management would identify the best prepared protective force personnel and then substitute them for lesser prepared personnel who were scheduled to participate in an exercise.

- Protective force members who would normally relieve other protective force personnel for the purposes of physical training, medical appointments, or sick leave would be armed and held in "stand-by" to participate in an exercise. This would potentially result in six or seven additional available armed responders that would not normally have been available during a shift.

  During our inspection, we learned that a Wackenhut official had recently acknowledged to a senior Department official that, as cited above, stand-by personnel had been used in performance tests in the past. We were told, however, that Wackenhut management had established new procedures to address this issue after becoming aware of it sometime in late 2000 or in 2001. One new procedure, for example, involves taking a figurative "snapshot" of the locations of protective forces at a given time, and starting an exercise with personnel stationed at the locations identified in the "snapshot."

- In an exercise in late 2000 or early 2001, protective force management told protective force responders the building and target to be attacked, the exact number of adversaries, and the location where a diversion would occur. This information was reportedly provided about three weeks before the exercise occurred, which allowed the protective force to formulate special plans on how to counter the adversary.

- For the June 26, 2003, exercise discussed in the prior section, after the first scenario had been run, word of the order of the attacks on the other three scenario targets spread among the lower ranked personnel. This was despite the fact that the specific order of the targets for this exercise was controlled information.

Although not all of the examples of alleged improper actions that were provided to us were attributed to specific individuals, two Wackenhut employees were identified as having been involved in such activities. When asked about the allegations, these individuals said that they had never provided controlled information to protective force personnel. They said that Wackenhut focused its training on those areas at Oak Ridge that present the greatest vulnerabilities, which also are the focus of performance tests. They further said that a Wackenhut employee who is not aware of these targeted preparations might conclude that controlled information had been provided. Regarding the MILES gear allegations, one of the individuals said he was aware that a number of years ago protective force personnel had tampered with the equipment, but when someone was caught doing this, corrective actions were taken. The other individual said he had heard stories of equipment tampering, but he had no first-hand knowledge.

As noted previously, protective force performance tests must be used to realistically evaluate and verify the effectiveness of protective force programs. Applicable policies and procedures require that the contents of the scenarios to be used in performance test exercises be controlled on a need-to-know basis. Although none of the individuals we interviewed had documentation to support their testimony that inappropriate actions occurred in connection with the protective force performance tests conducted at the Oak Ridge complex since the mid-1980's, the extent and nature of the testimonial evidence was so compelling that we

concluded that further action by management is needed if the credibility of the performance testing regime is to be maintained.

PERFORMANCE MEASUREMENT

As part of implementing GPRA, the Department is required to establish program goals and subsequently measure performance against those goals. We found that the contract between Wackenhut and DOE contained a performance objective and performance measure to address the efficacy of the protective force program. The performance objective required Wackenhut to execute a day-to-day protective services program that achieves the required level of protection, and the performance measure requires that optimum protective services support is provided in concert with site-specific needs. There is a Performance Evaluation Plan that is used for determining Wackenhut's award fee, and it establishes the criteria for Wackenhut to receive award fees.

We noted that in order to receive all fees that have been otherwise earned, Wackenhut must meet all DOE regulations. Given this performance standard and based on the information developed during the inspection, we believe that the results of the OIG review should be considered when DOE officials evaluate Wackenhut's contractual performance and award fee.

Also, our review of the test process at Oak Ridge disclosed that in addition to participating in the actual performance tests as the facility responder force, Wackenhut personnel also participated in the detailed planning and development of the tests. We believe that DOE officials should examine the extent to which a site protective force contractor should be involved in both these aspects of performance testing. Specifically, we believe that the Department should implement additional "firewalls" (controls) to ensure that responders do not receive inappropriate advance information that could undermine the integrity of a performance test.

RECOMMENDATIONS

We recommend that the Manager, Y-12 Site Office, and the Manager, Oak Ridge Operations Office:

1. Evaluate the information disclosed by our review and take appropriate action to ensure the integrity and realism of future performance tests.

2. Evaluate whether the information disclosed by our review impacts any previous analysis of the efficacy of the site's protective force, and take appropriate corrective actions.

3. Consider the information disclosed by our review when evaluating Wackenhut's performance, and take appropriate action with respect to determining award fee.

4. Evaluate whether it is appropriate for the same contractor to be responsible for both planning and participating as a protective force in protective force performance tests. Further, identify and implement additional safeguards to ensure that responders do not receive inappropriate advance information that could undermine the integrity of a performance test.

We recommend that the Director, Office of Independent Oversight and Performance Assurance:

5. Review the information provided in this report, and take action to ensure the integrity and realism of future performance tests at Y-12 and other Department facilities.

MANAGEMENT COMMENTS

NNSA concurred with our findings and recommendations and provided a series of corrective actions that either had been initiated or were planned as a result of direction from the NNSA Administrator and the Y-12 Site Office Manager. NNSA's comments, which are provided in their entirety at Appendix B to this report, also represent the position of the Oak Ridge Operations Office. The Office of Independent Oversight and Performance Assurance concurred with our recommendation to that Office. Comments from that Office are also appended to this report.

INSPECTOR COMMENTS

We found management's comments to be responsive to our recommendations.

Appendix A

SCOPE AND METHODOLOGY

We reviewed certain aspects of protective force performance tests at the Department's Oak Ridge Complex. The inspection fieldwork was conducted primarily from July through August 2003. We identified and reviewed applicable DOE regulations and other key documents applicable to the inspection. We interviewed Federal and contractor staff assigned to Department Headquarters and field locations in Oak Ridge, Tennessee, and Albuquerque, New Mexico. We also interviewed former contractor employees. We worked closely with the OIG Office of Investigations and the U.S. Attorney's Office for the Eastern District of Tennessee. We reviewed several relevant JCATS computer scenarios. This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

JAN 2 2 2004

MEMORANDUM FOR Alfred K. Walter
Acting Assistant Inspector General
for Inspections

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Draft Y-12 Protective Force Performance Improprieties Inspection Report

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review and comment on the Inspector General's (IG) draft Inspection report "Protective Force Performance Test Improprieties."

NNSA generally agrees with the report and concurs with the recommendations provided in the draft Inspection report and the separate draft Inspection report to management.

As you point out in your report the Y-12 site manager requested your office to conduct the subject review based on concerns that he had following completion of security exercises in summer, 2003. We appreciate the efforts of your office in conducting a review of the circumstances of those exercises. We consider the security of our nuclear complex to be one of our most critical responsibilities and your report will be very helpful in that regard. Y-12 security matters are of particular interest to NNSA currently and the Administrator has taken substantial additional steps to ensure we can be confident in our security program effectiveness there. Specifically, he has tasked the site manager and the Acting Chief Defense Nuclear Security to give disproportionate focus on Y-12 security matters in the coming months to provide necessary emphasis on all security activities at Y-12. In addition to focusing on the results of the recently completed inspection by the Office of Independent Oversight and Assurance, such attention will also include review of specifics of the circumstances which resulted in your recommendations. Further, we support your recommendation for a review of this matter by the Office of Independent Oversight and Assurance. Security performance testing by our NNSA sites is a key element in understanding how well sites are prepared to address potential threats to our national security assets. If such testing were in any way compromised so as to skew the quality of information we have about our ability to protect, the results could have extremely

Printed with soy ink on recycled paper

significant effects in a way which is entirely unacceptable. We will take all appropriate steps to ensure that is not the case.

I have attached the specific comments related to the recommendations. Should you have any questions related to this response, please contact Richard Speidel, Director, Policy and Internal Controls Management. He may be reached at 202-586-5009.

Attachment

cc: Dr. Everet Beckner, Deputy Administrator for Defense Programs, NA-10
William Brumley, Manager, Y-12 Site Office
David Marks, Field Chief Financial Officer, SvcCen/NV

Y-12 Site Office Responses to
Office of Inspector General Draft Inspection Report
"Protective Force Performance Test Improprieties"

Revision 3

Primary Draft Report

Recommendation 1 – Evaluate the information disclosed by our review and take appropriate action to ensure the integrity and realism of future performance tests.

Management Response – Concur. As a result of the findings cited in this investigation, continuous coordinated effort among the Y-12 Site Office, Wackenhut Services, Inc. (WSI) and BWXT Y-12, LLC (BWXT Y-12) has occurred to identify actions not already in-place that may be required to ensure the reliability and realism of future performance tests. In addition to analyzing the propriety of the events specifically associated with the Diagnostic Evaluation Exercise held on June 26, 2003, alleged examples of improper actions that were provided to the Office of Inspector General (OIG) by current or former protective force personnel will also be a focus of examination.

Recommendation 2 – Evaluate whether the information disclosed by our review impacts any previous analysis of the efficacy of the site's protective force, and take appropriate corrective actions.

Management Response – Concur. Analyses based on the new Design Basis Threat Policy characterize the current BWXT Y-12 security posture without reliance on any performance testing performed before July 2003. Y-12 has evaluated this data carefully to ensure that it is not relied on to select improvement initiatives without other supporting information. Therefore, the performance test held in June 2003, does not affect the current assumptions in the BWXT Y-12 security posture. The integrity of future testing to ensure the security posture, as well as safety and effectiveness, continues to be of utmost importance. To eliminate any confusion and avoid the perception of impropriety, test plans and procedures will be developed to ensure clarity of test expectations and roles and responsibilities of individuals who plan and participate in performance test exercises.

Recommendation 3 – Consider the information disclosed by our (OIG) review when evaluating Wackenhut's performance, and take appropriate action with respect to determining award fee.

Management Response – Concur. Among other factors, the soundness of all activities performed by WSI, and/or any other contractors, will continue to be a significant consideration in the award fee process for WSI. However, consideration of alleged improper actions referenced prior to WSI assuming the contract in January 2000, would not be appropriate in the determination of fee allowance during the remaining years of the WSI contract. As pointed out in the report, the examples of alleged improper actions

were obtained as the result of testimonial information from current and former protective force personnel and could not be substantiated by written documentation. The alleged actions were reputed to have occurred during a period when several different contractors were contractually responsible for safeguard and security activities at the Y-12 site. With the exception of the June 26, 2003, performance test, the specific dates of exercises for which allegations of improper actions occurred were not provided. Notwithstanding, the alleged impropriety of each action cited in the report will be examined, and corrective actions will be developed and implemented for those deemed improper.

Recommendation 4 – Evaluate whether it is appropriate for the same contractor to be responsible for both planning and participating as a protective force in protective force performance tests and what additional controls can be established to ensure that defenders do not receive inappropriate advance information that could undermine the integrity of a test.

Management Response – Concur. We will continue to evaluate the roles of each Contractor in the planning and participation phases of all performance tests. Separation of duties alone between contractors can not ensure that information is inappropriately disseminated or that the validity of a test is not undermined but will go far in improving confidence that our information is not shared. Y-12 will achieve proper conduct of security performance testing through clear expectations, integrity, accountability, and the development, implementation, and enforcement of performance test procedures. Those procedures will clarify roles and responsibilities of Contractor employees involved in performance tests including the sharing of information between Contractors.

Recommendation 5 – Review the information provided in this report, and take action to ensure the integrity and realism of future performance tests at Y-12.

Management Response – This response is to be provided by the Director, Office of Independent Oversight and Performance Assurance.

[Due to Privacy Act considerations, information that was provided herein that was responsive to recommendations contained in the separate report referenced on page 4 of this report are only being included in that report.]

Department of Energy

Oak Ridge Operations Office
P.O. Box 2001
Oak Ridge, Tennessee 37831—

January 21, 2004

Mr. David H. Sumner
Inspector General Eastern Regional Office
105 Mitchell Road
Oak Ridge, TN 37830

Dear Mr. Sumner:

CONCURRENCE ON INSPECTOR GENERAL RESPONSE, "PROTECTIVE FORCE PERFORMANCE TEST IMPROPRIETIES"

The Office of Inspector General (OIG) Report and recommendations concentrated on performance tests conducted at the Y-12 National Security Complex. However, since the Oak Ridge Operations (ORO) portion of the Wackenhut Services, Inc. (WSI) contract is a mirror of the Y-12 portion, the intent of the recommendations is also valid for the ORO portion of the contract. A representative of the ORO Office of Safeguards and Security (OSS) participated in review of the OIG Report and development of the Y-12 response. The one response appropriately incorporates the view of ORO OSS.

Sincerely,

Don F. Thress, Jr., Acting Director
Office of Safeguards and Security

Department of Energy
Washington, DC 20585

December 8, 2003

MEMORANDUM FOR: Alfred K. Walter
Acting Assistant Inspector General, IG-44

FROM: Glenn S. Podonsky, OA-1

SUBJECT: Comment on Draft Inspection Report on "Protective Force Performance Test Improprieties"

The Office of Independent Oversight and Performance Assurance (OA) concurs with the recommendation in your report, "Protective Force Performance Test Improprieties," November 2003, that OA ensure the integrity and realism of future performance tests at Y-12. As you may know, OA conducts tactical performance testing as a routine inspection activity, to include the ongoing inspection at Y-12. For this reason, OA has developed an extensive series of protocols to ensure the integrity of the outcome of such performance testing. These protocols include the following measures:

- The total number of site personnel (DOE and contractor) who are permitted insight into test scenarios prior to the conduct of the tests is strictly limited to those individuals essential to the preparation and presentation of safe, meaningful, and realistic tests.
- Site personnel who are permitted this insight are designated as "trusted agents" and are required to execute a trusted agent agreement that explicitly establishes restrictions on the communication of scenario information.
- OA controls the initiation of each individual test to minimize the impact of potential inadvertent or partial compromise. Specifically, site protective force personnel are pre-positioned in accordance with a predetermined "snapshot in time" and are held in that position until the onset of adversary actions, thus precluding artificial anticipatory movement of the protective force to target locations.
- OA details a cadre of independent evaluators to monitor the full range of performance test actions. These evaluators are trained to recognize actions that might compromise the results of the test (such as obscuring laser harness receptors).
- OA also conducts a detailed review of computer information recording "hits" resulting from laser engagements. Anomalies arising during this review are subject to follow up investigation.
- OA force-on-force performance testing is designed to support the evaluation of protective force performance against a range of evaluation criteria involving individual and team tactics, command, control, and communication, and other performance elements. It is not designed to support a simplistic "win/lose" outcome; as such, it is significantly less amenable to scenario compromise.

Printed with soy ink on recycled paper

In addition to these specific control measures, it should be noted that OA inspections address both the results of the performance tests and also the demonstrated ability of the site to conduct fair and objective performance tests. Although OA's recent experience is that site personnel do not attempt to deliberately compromise performance tests during inspections, we are always vigilant in considering the possibility of such compromise, and would consider validated instances of such activity as a significant weakness of the protective force management and performance.

Should you need additional information, please contact me at (301) 903-3777, or Arnold E. Guevara, Director, Office of Safeguards and Security Evaluations, at (301) 903-5895. We appreciate the opportunity to comment on this report.

Glenn S. Podonsky, Director
Office of Independent Oversight
and Performance Assurance

cc:
G. Friedman, IG-1
R. Speidel, NA-66
M. Kilpatrick, OA-1
A. Guevara, OA-10

IG Report No. DOE/IG-0636

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

8

Richard J. Levernier
P.O. Box 146
Germantown, MD 20875

August 26, 2005

Catherine A. McMullen, Esq.
Chief, Whistleblower Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, NW
Washington, DC 20036

Via Certified Mail # 7099 3400 0005 4288 5578

Dear Ms. McMullen:

This is in response to your letter of August 12, 2005, concerning my whistleblower disclosure to the United States Office of Special Counsel (OSC). The purpose of this letter is to provide comments on the Department of Energy (DOE) redacted report concerning my whistleblower disclosure. On January 15, 2002, I submitted a whistleblower disclosure to the OSC (File No. DI-02-0572). On October 25, 2002, the OSC determined that there was a "substantial likelihood" that the information contained in my disclosure constituted a substantial and specific danger to public health and safety arising out of actions taken or not taken by officials at DOE concerning physical security at DOE's nuclear weapons facilities. Therefore, OSC transmitted the allegations to the Secretary of Energy for an investigation and report pursuant to 5 USC 1213 (c). Pursuant to the statute, the Secretary had 60 days to conduct an investigation of these allegations and report back to OSC.

On May 29, 2003, the Secretary of Energy submitted the required report of investigation to OSC. On December 2, 2003, I was contacted by OSC, through my legal counsel, and informed that the DOE report (25 pages in length) was ready for my review. The report was available to me only (not my legal counsel) at OSC due to restrictions imposed by DOE. On December 19, 2003, I submitted my initial comments on the DOE report concerning my whistleblower disclosure to OSC (copy attached).

Subsequent to submittal of my comments, on January 23, 2004, the DOE Office of the Inspector General (OIG) issued an inspection report, *Protective Force Performance Test Improprieties* (DOE/IG-0636; this OIG report and all other OIG reports referenced herein are available on the DOE OIG website at http://www.ig.doe.gov/) which is directly relevant to my whistleblower disclosure since cheating on protective force performance tests was one of the central issues referred by OSC to DOE for investigation. On February 10, 2004, I provided additional comments on the DOE investigation of my whistleblower disclosure (copy attached).

I appreciate the opportunity to provide comments on the redacted DOE report which will become part of the public file on this matter. The comments I provided on December 19, 2003 and February 10, 2004 are still applicable and relevant. I requested the opportunity

to review the OSC referral of my whistleblower disclosure to DOE in order understand how my issues were framed by OSC for DOE investigation. My initial request to review the OSC referral was ignored. Please explain the legal authority and public policy basis under the Whistleblower Protection Act and 5 USC 1213 for the OSC to keep secret from me the way OSC translated my charges and which it deemed worthy of investigation.

It is very interesting to note that although the DOE concluded the allegations were unfounded significant new and additional evidence to the contrary from DOE's own OIG exists. In November 2004 the DOE OIG issued a Special Report, *Management Challenges at the Department of Energy* (DOE/IG-0667). The Background section of the report states, "In 1997, the Office of the Inspector General began an annual effort to identify what it considers to be the most significant management and performance challenges facing the Department of Energy. Now codified as part of the *Reports Consolidation Act of 2000,* this effort highlights those programs and operations that are, in our judgment, inherently the most difficult to manage and those with **demonstrated performance problems**".

The Results section of the report states, "In our previous report, *Management Challenges at the Department of Energy* (DOE/IG-0626, November 2003), we identified six management challenges. The Department has taken significant positive steps to address these challenges; however, we concluded that these challenges continue as the most serious risks facing the Department in 2005 and beyond. Each of these challenges has been a long standing and widely acknowledged issue for the Department of Energy. Mission-Related Challenges: National Security; Environmental Cleanup; Stockpile Stewardship."

The National Security section of the report states, "As in previous years, we have identified national security as a significant management challenge due to both the criticality of the Department's operations and the continuing nature of security threats. The Department must ensure that its sensitive materials, facilities, and information are secure and protected from hostile groups or countries... Further, the Department and its contractors rely upon protective force personnel to secure and protect facilities that produce, store, and handle significant quantities of nuclear materials, weapons, and national security-related information. Our reviews concerning the readiness of the Department's protective forces identified needed improvements at sites that represent some of the most critical national security components in the Department's complex. In our inspection report on *Protective Force Performance Test Improprieties* (DOE/IG-0636, January 2004) we confirmed the concerns of a site manager that that the results of a protective force performance test conducted in June 2003 may have been compromised and, in our opinion, should not be relied upon. Our audit of *The Department's Basic Protective Force Training Program,* (DOE/IG-0641, March 2004) found that the Department's standardized, basic protective force core training curriculum had been applied inconsistently throughout the complex. While some level of deviation from the core training curriculum to meet local conditions was understandable, the relatively large number of curriculum modifications identified during the audit raised concern as to the curriculum's validity and usefulness as a benchmark for evaluating the performance of protective force training. In our inspection report on *Reporting of Security Incidents at the Lawrence Livermore National Laboratory* (DOE/IG-0625, November 2003), we

concluded that Livermore did not ensure security incidents involving missing master keys and master Tesa cards were reported within required timeframes, nor were timely follow-up actions taken to identify and address potential security vulnerabilities resulting from the incidents."

The DOE OIG inspection report *Protective Force Training at the Department of Energy's Oak Ridge Reservation* (DOE/IG-0694, June 2005) Results of Inspection section stated, "Our inspection confirmed the essence of the facts presented in the allegation. Of greater importance, we concluded that there were material shortcomings in the implementation of the protective force training program at the Oak Ridge Reservation. Specifically, we found that:

- Protective force personnel spent, on average, about 40 percent less time on combat readiness refresher training than that specified in the approved Fiscal Year 2004 training plan;
- For some personnel, planned training time was formally reported to the Department as actual training time, resulting in an overstatement of the training received;
- Protective force personnel at the Y-12 National Security Complex routinely worked in excess of 60 hours per week, despite a 60 hour maximum threshold for safe operations established by the Department of Energy Protective Force Program Manual. There was evidence that working excessive overtime negatively impacted the ability or willingness of some protective force personnel to complete the required physical fitness training; and,
- Some protective force personnel signed attendance rosters for on-the-job refresher training without receiving the training."

The Inspector Comments section of the report stated, "Management's comments indicated a fundamental disagreement on the core issues in our report. We carefully considered the positions asserted by management and did not find them compelling."

The DOE OIG inspection report, *Security Access Controls at the Y-12 National Security Complex* (DOE/IG-0691, June 2005) Results of Inspection section stated, "We found that foreign construction workers, using false documents, had, in fact, gained access to the Y-12 site on multiple occasions. Specifically, 16 foreign construction workers were found to have been illegal aliens. Some of these workers acquired facility access badges and were, as a result, permitted access to the main Y-12 site. Others were able to access an adjacent Y-12 leased facility. Further, certain information associated with the construction of the Y-12 leased facility, which was planned to store document classified up to Secret-Restricted Data, was considered Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO)."

The Inspector Comments section of the report stated, "NNSA has policies in place to control access at Y-12 and other NNSA sites. These policies failed to prevent the deficiencies we identified at Y-12. In that regard, the effective implementation of not only the corrective actions at Y-12, but the implementation of Presidential Directive 12

throughout the DOE complex, takes on greater importance. NNSA pointed out that there was no evidence that foreign nationals with fraudulent green cards had access to UCNI or OUO documents. During our physical inspection of the Y-12 leased facility, we observed UCNI and OUO documents lying unprotected in a construction trailer, which was accessed by the foreign construction workers who are the subject of this report. Thus, these individuals were afforded opportunities to access UCNI, as well as OUO information. We concluded that this situation represented a potentially serious access control and security problem."

The DOE OIG inspection report *Security and other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory* (DOE/IG-0677, February 2005) Background Section of the report stated, "Los Alamos National Laboratory (LANL), as part of the National Nuclear Security Administration (NNSA), contributes to meeting the Nation's nuclear deterrence capability and other security needs. LANL is operated by the University of California (UC) and is one of the Department of Energy's most sensitive sites. The laboratory directly employs about 7,500 UC employees, of which approximately 800 terminate their employment each year."

The Results of Inspection section of the report stated, "LANL out-processing procedures were not followed by more than 40 percent of the 305 terminating employees included in our sample. Consequently, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating. Given this and the results of additional sampling, we found that there was no assurance that, prior to departure, LANL terminating employees turned in security badges, completed the required Security Termination Statement, or had their security clearances and access authorizations to classified matter and/or special nuclear material terminated in a timely manner. To illustrate, of a sample of 96 cleared employees who departed LANL over a 2-year period:

- Forty-four employees had not turned in their badges at the time of our field work;
- Sixty-one employees did not complete the Security Termination Statement at the time of their departure;
- Twenty-one employees retained their clearances in the Department's official database from 11 to 567 days after their departure; and,
- One employee retained his sensitive compartmented information authorization for more than 5 months after his retirement."

The Management Comments section of the report stated, "However, NNSA disagreed with our characterization of the seriousness of the consequences resulting from the lack of adherence to established out-processing procedures, and NNSA believed it was more accurate to state there was a potential for unauthorized access."

The Inspector Comments section of the report stated, "We found management's comments to be generally responsive to our report. However, we disagree with NNSA's position regarding the seriousness of the issues raised in this report. The integrity of the

Department's security program is built on the premise that only authorized persons have access to classified and sensitive information."

It is important recognize that the loss of the national assets entrusted to DOE would have truly catastrophic consequences and make the events of 9/11 pale in comparison. In June 1999 the President's Foreign Intelligence Advisory Board (PFIAB) issued *Science at its Best/Security at its Worst* (http://www.fas.org/sgp/library/pfiab/) which states, "At the birth of DOE, the brilliant scientific breakthroughs of the nuclear weapons laboratories came with a troubling record of security administration. Twenty years later, virtually every one of its original problems persists...The Department has been the subject of a nearly unbroken history of dire warnings and attempted but aborted reforms. A cursory review of the open source literature on the DOE record of management presents an abysmal picture. Second only to its world-class intellectual feats has been its ability to fend off systemic change. Over the last dozen years, DOE has averaged some kind of major departmental shake-up every two to three years. No President, Energy Secretary, or Congress has been able to stem the recurrence of fundamental problems. All have been thwarted time after time by the intransigence of this institution. The Special Investigative Panel found a large organization saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial... Time after time over the past few decades, officials at DOE headquarters and the weapons labs themselves have been presented with overwhelming evidence that their lackadaisical oversight could lead to an increase in the nuclear threat against the United States. Throughout its history, the Department has been the subject of scores of critical reports from the General Accounting Office, the intelligence community, independent commissions, private management consultants, Its Inspector General, and its own security experts. It has repeatedly attempted reforms. Yet the Department's ingrained behavior and values have caused it to continue to falter and fail."

In conclusion, I continue to believe that the scope and magnitude of security problems at DOE, which were identified in my whistleblower disclosure almost 4 years ago, constitute a substantial and specific danger to public health and safety. Given the significant increases in the terrorist threat which has been universally acknowledged since 9/11, the degradation of national security that results from these deficiencies is even greater now. I believe that any objective and reasonable person evaluating my whistleblower disclosure, the DOE investigative report concerning my whistleblower disclosure and subsequent directly relevant U.S. General Accounting Office (GAO) and DOE OIG reports and testimony will find the DOE report seriously lacking in credibility. I also believe the information contained in the GAO testimony referenced in my December 19, 2003, comment letter to OSC, i.e. that DOE will likely not have the financial resources necessary to address the May 2003 DBT until fiscal year 2006, and that it will take an additional 2 to 5 years to implement the required additional security measures, creates an extended window of vulnerability and exacerbates an already unsatisfactory situation. Given that DOE is protecting nuclear weapons and special nuclear materials and recognizing the catastrophic consequences associated with a security breach, only the highest level of protection is acceptable. Uncertainty about DOE's ability to protect nuclear weapons and special nuclear material is unacceptable. Until DOE abandons its longstanding approach of denial for any alleged security problems, our nation will continue to be vulnerable to preventable terrorist threats.

DOE's denial mentality for security deficiencies is clearly apparent with respect to cheating on performance tests. I identified systemic cheating on protective force performance tests at DOE nuclear weapons facilities in my whistleblower disclosure. The DOE investigation of my whistleblower disclosure determined that all of my allegations were unfounded and the Secretary of Energy signed a letter containing that false conclusion to the Special Counsel. Shortly thereafter the DOE OIG issued a formal Inspection Report concluding there has been a pattern of cheating on protective force performance tests going back to the mid-1980's. In several recent instances cited above the OIG documented in the Inspector Comments sections of reports their disagreement with the official DOE denial of their findings. The OIG stated they did not find the defensive positions taken by DOE/NNSA management to be compelling. In another instance where the OIG found sensitive UCNI and OUO documents lying unprotected in an area with unauthorized foreign nationals present the DOE management reaction focused on the assumption that there was no evidence that the information had been compromised. Common sense dictates that successful spys do not leave calling cards. This type of bureaucratic denial mentality in the face of obvious information to the contrary has been determined to be a major contributing factor to the security failures that resulted in tragic events of 9/11. The protection of critical national security assets, especially special nuclear material (SNM) and weapons, in the custody and control of the DOE is not a game. The loss of nuclear weapons or SNM would have catastrophic consequences and clearly constitutes a substantial and specific risk to public health and safety. Unless OSC or Congress takes immediate action on this matter, this significant national security vulnerability will continue unabated and ripe for terrorist exploitation.

I appreciate the opportunity to provide additional comments to OSC on this matter. Please contact me at (301) 903-2178 if you have any questions, or through my attorney Tom Devine at (202) 408-0034, ext.124. I will be out for the next two weeks, but then request an opportunity to meet with and brief you on the ongoing, dormant threats to homeland security that this report is endorsing. That would be a responsible measure on your part, before publicly announcing that DOE has reasonably addressed my concerns by denying them all.

I hope that you want to prove you want to know by hearing me out, because at this stage the OSC whistleblowing process has lost its credibility as a way to make a difference protecting homeland security. So far the current exercise is an empty rerun. Unlike the prior administration, neither you nor your staff engaged in any meaningful communications with me since February 2004 when I turned in my supplemental comments. Now you have given me a chance to resubmit my comments on the identical report that the OSC first showed me in December 2002. Please explain the legal basis under the Whistleblower Protection Act to withhold an unclassified report transmitted under 5 USC 1213 from the public record for over two years. This has prevented timely public review and scrutiny of homeland security threats that remain unaddressed. Blowing the whistle has been a highly painful experience for me, a duty I pursued at great cost to my career. As the previous Special Counsel's prohibited personnel practice investigation confirmed, I was suspended, lost my security clearance – which still has not

been restored -- and exiled from my professional expertise – for raising these issues. I risked and endured this retaliation in order to make a difference, not to be window dressing.

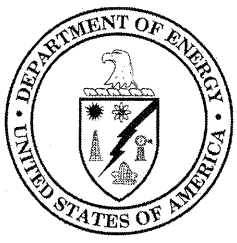
Sincerely,

Original Signed by Richard J. Levernier

Richard J. Levernier

Attachments (2)

9



U.S. Department of Energy
Office of Inspector General
Office of Inspections

Inspection Report

Reporting of Security Incidents at the Lawrence Livermore National Laboratory

DOE/IG-0625

November 2003

Department of Energy

Washington, DC 20585

November 4, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Reporting of Security Incidents at the Lawrence Livermore National Laboratory"

BACKGROUND

The Department of Energy's (DOE) Lawrence Livermore National Laboratory (Livermore) performs research and development activities that require the highest levels of security. On May 5, 2003, Livermore officials reported to DOE that a set of master keys had been discovered missing on April 17, 2003. On May 30, 2003, Livermore officials reported to DOE that a master Tesa card, which is a plastic card-like key with a magnetic strip, had been discovered missing on April 12, 2003. The loss of the master keys and Tesa card, and the delay in reporting these losses, raised the possibility of security vulnerabilities at the Laboratory. The purpose of this inspection was to determine the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as missing master keys and master Tesa cards, and the identification and correction of corresponding potential security vulnerabilities.

RESULTS OF INSPECTION

We concluded that Livermore did not have adequate internal controls to ensure that: (1) security incidents involving missing master keys and Tesa cards were reported within required timeframes, and (2) that timely follow-up actions were taken to identify and address any potential security vulnerabilities resulting from the incidents. Specifically, we found that Livermore security officials:

- Misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card;

- Did not report the security incidents involving the missing master keys and master Tesa card to DOE within required timeframes;

- Did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card; and

Printed with soy ink on recycled paper

- Did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

During our review we learned that during a May 2003 inventory, Livermore officials identified an additional three master keys and two master Tesa cards that were missing. Although two of the three master keys had been reported missing by the Livermore Fire Department to the Protective Force Division more than three years before, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. Recent DOE and Livermore oversight reviews of Livermore's safeguard and security operations did not identify internal control weaknesses related to the control and inventory of master keys and master Tesa cards.

As a result of the potential security vulnerabilities caused by the missing master keys, Livermore eventually initiated actions to replace or upgrade locks at significant cost. Livermore officials initially estimated the cost to replace or upgrade the locks as $1.7 million. This figure was challenged upon release of our draft report. However, as of the date of this report, officials of the National Nuclear Security Administration (NNSA) have not provided a different cost figure. Ultimately, Federal taxpayers will bear this cost. We believe that Livermore failed to ensure compliance with established internal controls over the master keys and master Tesa cards, and as such, we question the allowability of these costs.

MANAGEMENT REACTION

Management did not specifically state concurrence with our recommendations. However, management identified corrective actions that NNSA believes are responsive to our recommendations. These actions include implementing additional procedures and training.

Although this is a good first step, management needs to do more to assure that Livermore places greater emphasis on the need to strictly follow its processes and procedures for accountability and control of security keys. Management stated that such processes are captured in site security surveys and self-assessments, but acknowledged that they were not followed in these cases. Similarly, an October 14, 2003, press article reported that a gate to a limited security area at the Laboratory, a secured facility, was left unlocked. In our view, this latest incident only serves to reinforce the need for greater commitment by Laboratory management and personnel to prevent security incidents, and when they occur, to report and resolve them promptly.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Manager, Livermore Site Office
Director, Policy and Internal Controls Management

REPORTING OF SECURITY INCIDENTS AT THE LAWRENCE LIVERMORE NATIONAL LABORATORY

TABLE OF CONTENTS

OVERVIEW

Introduction and Objectives 1

Observations and Conclusions 2

DETAILS OF FINDINGS 4

Reporting Thresholds for Security Incidents 4

Reporting Security Incidents to DOE/NNSA 5

Additional Missing Keys 6

Security Risk Assessments 7

Compensatory Measures 7

Performance Measures 9

Oversight Reviews 9

RECOMMENDATIONS 10

MANAGEMENT COMMENTS 11

INSPECTOR COMMENTS 12

APPENDICES

A. Scope and Methodology 13

B. Management Comments 14

Overview

INTRODUCTION AND OBJECTIVES

Lawrence Livermore National Laboratory (Livermore) performs research and development activities in support of national defense that require the highest levels of security. The University of California (UC) manages and operates Livermore under contract with the Department of Energy (DOE), which includes the National Nuclear Security Administration (NNSA).

On May 13, 2003, Livermore officials issued a Press Release stating that a set of master keys assigned to a Livermore Protective Force Officer had been discovered missing on April 17, 2003. Later, on May 30, 2003, a Livermore official announced to employees that a master Tesa card, which is a plastic card-like key with a magnetic strip, had been discovered missing on April 12, 2003.

Keys and electronic entry cards are an essential component of the system of access controls at Livermore and other DOE sites. Unique keys and cards, by their nature, serve to restrict access by unauthorized individuals to specific areas that may contain classified information and materials, sensitive program, project or proprietary information, or the personal belongings of Laboratory employees. Master keys and cards, on the other hand, control access to a significant number of the facilities, buildings and offices at Livermore. Their distribution is restricted to a limited number of personnel in order to ensure the integrity of the unique key and card access control component.

The objectives of this inspection were to determine: (1) the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as the missing master keys and master Tesa cards, and the identification and correction of corresponding potential security vulnerabilities; and (2) if performance measures exist at Livermore that adequately address the reporting of such incidents.

OBSERVATIONS AND CONCLUSIONS

We concluded that Livermore did not have adequate internal controls to ensure that security incidents involving missing master keys and master Tesa cards were reported within required timeframes, and that timely follow-up actions were taken to identify and address potential security vulnerabilities resulting from the incidents.

Specifically, we found that Livermore security officials:

- Misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card;

- Did not report the security incidents involving the missing master keys and master Tesa card to DOE/NNSA within required timeframes;

- Did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card; and

- Did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

During our review we learned that Livermore officials initiated a complete inventory in May 2003, to determine the status of all master keys and master Tesa cards at Livermore. The inventory disclosed that an additional three master keys and two master Tesa cards were missing. This brought the total number of missing master keys to nine, and the total number of missing master Tesa cards to three. Two of the three missing master keys were from a set of keys that the Livermore Protective Force Division set aside for use by the Livermore Fire Department. A Fire Department official told us that the two master keys had been reported missing to the Protective Force Division over three years ago. However, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. We were told that at that time, the view of the Protective Force Division was that the set of keys contained fewer master keys than were typically found on other sets of keys, not that any master keys were missing.

Although keys and cards are only one component of the system of access controls at Livermore, the loss of the master keys and master Tesa cards affected the level of security afforded classified and sensitive areas at Livermore. As a result of the potential security vulnerabilities caused by the missing master keys, Livermore eventually initiated actions to replace or upgrade locks at significant cost. We were initially advised by Livermore officials that the estimated cost to replace or upgrade the locks was $1.7 million. Commenting on our draft report, NNSA officials did not believe the cost estimate was consistent with the Laboratory's expenditures or numbers of locks to be replaced. However, as of the date of this report, NNSA officials had not provided a revised cost figure. Ultimately, Federal taxpayers will bear this cost. We believe that Livermore failed to ensure compliance with established internal controls over the master keys and master Tesa cards. Therefore, we question the allowability of these costs.

REPORTING THRESHOLDS FOR SECURITY INCIDENTS

We found that Livermore security officials misinterpreted fundamental DOE reporting requirements for security incidents, and did not immediately recognize the significant security implications of the missing master keys and master Tesa card.

Reporting Requirements

DOE Notice 471.3, "Reporting Incidents of Security Concern," establishes four reporting thresholds for incidents of a security concern under an Impact Measurement Index (IMI) system. The highest reporting threshold, IMI-1, is for "Any security incident that can be expected to cause serious damage to national security or DOE security interests." The lowest reporting threshold, IMI-4, is for "Any security incident that causes no damage to national security, but that can, in combination, indicate weakened security awareness or inadequate procedures or practices."

At Livermore, the Safeguards and Security Department's Office of Incidents and Infractions is the responsible entity for reporting security incidents to DOE in accordance with DOE Notice 471.3. This office relies, in part, on the Protective Force Division providing reports on individual incidents that have occurred at Livermore so that a reporting determination under DOE Notice 471.3 can be made.

A Livermore security official informed us that on two occasions immediately following the loss of the set of master keys on April 17, 2003, a review was conducted of the security incident reporting criteria. According to the official, the reviews did not identify a need to report the loss of the master keys to DOE. The official said that another Livermore security employee discussed the loss of the keys with Livermore's Office of Incidents and Infractions and was told by that office that the loss of the master keys did not require reporting to DOE. According to an employee in the Office of Incidents and Infractions, his review of the IMI reporting categories in the DOE Notice did not identify a specific reference to "missing master keys," but it was unclear in his mind whether or not the loss of the keys was reportable.

The loss of a master Tesa card on April 12, 2003, was not reviewed by the Office of Incidents and Infractions for reporting under DOE Notice 471.3 until the office received an Incident Report from the Protective Force Division on or about May 30, 2003. The loss of the master Tesa card was reported at that time as an IMI-4 incident.

Security Implications

Although the set of master keys and the master Tesa card opened locks leading to some of the most sensitive areas of the Laboratory, Protective Force Division officials did not perceive the loss as having the potential to cause damage to national security or DOE security interests. A Protective Force Division official advised us that they had lost keys before and that the keys had always turned up. The official told us that when the set of master keys did not turn up after a few days of extensive searching, the Protective Force Division became involved in other security issues and did not focus on the security implications of the missing keys. In addition, the official stated that the Protective Force Division was not aware that during the period that the master keys were missing, a master Tesa card was also missing. The Protective Force Division did not consider the security implications of the double failure[1] resulting from the two types of master keys (i.e., keys and Tesa card) being missing at the same time.

After Livermore senior management became aware of the missing master keys on May 5, 2003, the Office of Incidents and Infractions classified the incident at the lowest reporting threshold, IMI-4, that is, a security incident "that causes no damage to national security." It was not until the intervention of a senior NNSA official on May 9, 2003, that the Office of Incidents and Infractions re-evaluated the incident and reclassified it as an IMI-2, which is defined as "Any security incident that can be expected to cause damage to national security or DOE security interests."

REPORTING SECURITY INCIDENTS TO DOE/NNSA

We found that Livermore security officials did not report the security incidents involving the missing master keys and master Tesa card to DOE/NNSA within required timeframes.

DOE Notice

DOE Notice 471.3 states that a facility has 24 hours to determine if a security incident should be reported. If the incident should be reported, it must be categorized under the IMI system. The most serious category of security incidents, IMI-1, must be reported to DOE within one hour after categorization; IMI-2 and IMI-3 incidents must be reported within 8 hours; and summaries of IMI-4 incidents are to be reported monthly.

However, these incidents were not reported to DOE/NNSA until weeks after they were first recognized. Specifically:

- The master Tesa card discovered missing on April 12, 2003, was not reported to DOE/NNSA until May 30, 2003.

[1] A double failure occurs when the two primary types of security locks protecting the same area are compromised at the same time.

- The set of six master keys discovered missing on April 17, 2003, was not reported to DOE/NNSA until May 5, 2003.

We learned that Protective Force Division officials had no immediate plans of reporting the missing keys to Livermore management or DOE. A Protective Force Division official advised us that the issue of the missing keys was on a list of things to discuss with higher management, but the issue was never discussed. The missing keys went unreported until May 5, 2003, when an alert employee in the Livermore Locks and Keys Shop became aware of an attempt by the Protective Force Division to have a duplicate set of the master keys made to replace the missing set, and promptly alerted security officials in the Safeguards and Security Department of the missing master keys.

Similarly, the missing master Tesa card went unreported until May 30, 2003. Although the Protective Force Division Incident Report was dated April 12, 2003, the Office of Incidents and Infractions did not receive the report until an employee in the Safety, Security and Environmental Protection Directorate alerted senior Livermore management about the missing master Tesa card.

ADDITIONAL MISSING KEYS

We found that Livermore security officials could not determine how long other master keys and master Tesa cards had been missing.

In May 2003, Livermore security officials initiated a complete inventory to determine the status of all master keys and master Tesa cards. The inventory disclosed that an additional three master keys and two master Tesa cards were missing. Two of the three missing master keys were on a set of keys used by the Livermore Fire Department. A Fire Department official told us that the two master keys had been reported missing to the Protective Force Division over three years ago. However, the Protective Force Division took no action to inventory the keys or determine why the two keys were missing. At that time, the view of the Protective Force Division was that the set of keys contained fewer master keys than were typically found on other sets of keys, not that any master keys were missing.

The two missing master Tesa cards had been placed in storage by the Protective Force Division. The Protective Force Division could not locate the two master Tesa cards during the inventory.

Livermore security officials were unable to ascertain when the master keys and master Tesa cards were lost. Based on our review, we concluded that Livermore did not have adequate inventory

controls over its master keys and master Tesa cards. We consider such controls to be a fundamental part of the security regime at an institution like Livermore that is responsible for conducting highly classified and sensitive activities in support of national defense. Upon completion of the May 2003 inventory, Livermore officials notified DOE/NNSA of the additional missing master keys and master Tesa cards.

SECURITY RISK ASSESSMENTS

We found that Livermore security officials did not immediately assess potential security risks to identify vulnerabilities resulting from the missing master keys and master Tesa card.

The master keys were missing for over two weeks before any consideration was given to assessing potential security risks to identify possible vulnerabilities. On May 6, 2003, a Safeguards and Security Department official directed that a risk assessment be conducted, which included the most sensitive areas of the Laboratory. A Livermore Safeguards and Security Department official then directed the conduct of a second risk assessment that included national security assets such as classified matter, unclassified controlled nuclear information, high explosives, biological assets, Category IV Special Nuclear Material (SNM) and firearms.

The master Tesa card was missing for 32 days before a notification was made to Livermore program officials. On May 14, 2003, Safeguards and Security Department officials informed Laboratory program officials of the loss and the need for assessing potential security risks. During this meeting the security implications of the double failure were discussed for the first time, one month after the double failure condition occurred.

COMPENSATORY MEASURES

We found that Livermore security officials did not take timely compensatory measures to mitigate the potential vulnerabilities resulting from the missing master keys and master Tesa card.

Protective Force Division officials took no compensatory measures to address potential security vulnerabilities associated with the missing master keys and master Tesa card prior to May 6, 2003. A Protective Force Division official advised us that they were not aware of the double failure resulting from the combination of the missing master keys and master Tesa card until a meeting in early May 2003. However, the official said that compensatory measures should have been taken with respect to the missing master keys anyway. According to the official, the focus at the time was on finding the keys, and that when the keys were not found, their

focus changed to other protective force issues and they did not address the issue of compensatory measures.

Short-term compensatory measures, which were the result of intervention by Livermore management outside the Protective Force Division, were not initiated until May 6, 2003. These measures, which consisted of block-out blades, door seals, re-keying, suspension of the day-lock-rule[2], and installation of additional Tesa locks, were completed a month or more after the master keys and master Tesa card were discovered missing.

The dates of discovery of the respective missing master keys and master Tesa cards and the dates they were reported to DOE/NNSA as missing are shown in Figure 1.

Summary of Missing Master Keys and Tesa Cards

Type of Key	Date Missing	Date Reported
1 Master Tesa	April 12, 2003	May 30, 2003
6 Master Keys	April 17, 2003	May 5, 2003
2 Master Keys	3 or more years[3]	May 30, 2003
1 Master Key	Indeterminate Period	May 31, 2003
2 Master Tesa	Indeterminate Period	June 2, 2003

Figure 1

Corrective Action Plans

We were advised by an NNSA official that on June 12, 2003, the NNSA Livermore Site Office issued three major findings to Livermore related to security locks and keys. We were also advised that by July 2003, formal corrective action plans to correct vulnerabilities in security incident reporting and security key control and inventory procedures were in place. According to the NNSA official, Livermore has completed several corrective action plan milestones, which will be validated by the Livermore Site Office by the end of December 2003.

[2] The day-lock-rule allows classified materials to be left unattended for brief periods provided that other security measures (i.e. items secured in a locked room) are in place to prevent unauthorized access.

[3] Keys reported by the Livermore Fire Department as missing more than three years ago.

Cost of Lock Replacement

With reliance on a complex lock, key, and Tesa card security strategy at Livermore to prevent access to classified and sensitive areas, there is little doubt that the level of security afforded these areas was adversely affected. Livermore officials initially advised us that, in the long-term, the loss of the master keys would require the replacement and upgrade of approximately 100,000 locks in both classified and unclassified areas within 526 buildings. They also initially estimated the total cost of this lock replacement project, which also includes upgrading existing locks, at approximately $1.7 million. However, as of the date of this report, NNSA officials had not validated this figure as accurate.

UC is required by Clause I.062 of its contract with DOE to have methods and procedures in place to reasonably ensure that the mission and functions assigned to the contractor are efficiently and properly executed, and that resources are safeguarded against waste, loss, and mismanagement. As reported by an internal Livermore review team, Livermore violated its internal control procedures for the control and accountability of master keys. This resulted in the need to replace and upgrade locks, and take other compensatory measures. We were told that prior to the loss of the master keys in April 2003, no such lock replacement project had been planned. Based on Livermore's failure to exercise due diligence in performing its contractual responsibilities, we question whether these costs are allowable.

PERFORMANCE MEASURES

Our review of the contractor performance self-assessment criteria for Fiscal Year 2003 revealed that a specific statement to "Conduct analysis of [the] incident pertaining to key control and accountability" was added to the Livermore Safeguards and Security Assessment Management Plan in June 2003. We were told by a senior NNSA Livermore Site Office official that a Livermore self-assessment performance review of the results of Fiscal Year 2003 Safeguards and Security operations will be conducted and that it will include the missing key incidents detailed in this report.

OVERSIGHT REVIEWS

Recent DOE and Livermore oversight reviews of Livermore's safeguards and security operations prior to the disclosure of the missing master keys and missing master Tesa card, did not identify internal control weaknesses related to the control and inventory of master keys and master Tesa cards. Guides developed by various organizations to plan and conduct these reviews suggest that processes should be reviewed to determine whether procedures are in place to adequately control keys and locks. However, none of these oversight reviews identified the key control and inventory weaknesses at

Livermore that allowed master keys and Tesa cards to go missing for an extended period of time without detection.

Several security surveys and self-assessments performed by NNSA and Livermore since 2000 did not report any issues relating to key control and inventories. These reviews consistently rated topical areas that included key control and inventories as "satisfactory." Although a 2003 security survey verified the existence of lock and key records and procedures, the survey did not evaluate the accuracy or effectiveness of the records and procedures in controlling and accounting for keys.

In comments to our draft report, the NNSA Associate Administrator for Management and Administration stated that although NNSA believes the processes in place related to the security of keys are captured in the surveys and self-assessments, the established processes and procedures were not followed. He stated that NNSA will provide a copy of our recommendations and NNSA's expectations to the Site Office Managers for their inclusion in their respective oversight processes.

We believe that future field site security surveys and self-assessments should include a review of internal controls relating to the issuance, receipt, and inventory of keys that provide access to sensitive areas.

We noted that a 2002 DOE assessment of physical security systems at Livermore included a review of barriers protecting special nuclear material facilities. The missing master keys and Tesa cards accessed locks in some of these facilities. The assessment report was silent regarding whether master keys and Tesa cards were included in the review. However, Livermore physical security systems received a rating of "EFFECTIVE PERFORMANCE."

RECOMMENDATIONS

We recommend that the Administrator, National Nuclear Security Administration:

1. Ensure that field site security surveys and self-assessments include a review of internal controls relating to the issuance, receipt, and inventory of all keys involving sensitive areas.

We also recommend that the Manager, Livermore Site Office:

2. Review the costs incurred by Livermore to replace and upgrade approximately 100,000 locks necessitated by the missing master keys and master Tesa cards, to determine whether the costs are reasonable and allowable.

3. Ensure that Livermore establishes appropriate internal controls to correctly identify reportable incidents, and that such incidents are reported in a timely manner.

4. Ensure that Livermore officials responsible for categorizing incidents reportable under DOE Notice 471.3 are trained to properly determine the appropriate IMI classification level of security incidents.

5. Ensure that internal controls are established by Livermore that promote the timely assessment of vulnerabilities resulting from security incidents, and the prompt implementation of compensatory measures.

6. Ensure that Livermore has established appropriate internal controls for the management and inventory of master keys and master Tesa cards.

MANAGEMENT COMMENTS

In comments to our draft report, the NNSA Associate Administrator for Management and Administration stated that the report is consistent with the findings of Laboratory, Livermore Site Office, University of California and NNSA reviews of the security locks and keys incidents. While the Associate Administrator did not specifically state concurrence with our recommendations, he identified corrective actions taken by the Livermore Site Office and the Laboratory that he believed were responsive to our recommendations.

Regarding recommendation 1, the Associate Administrator acknowledged that while processes related to security of keys are captured in surveys and self-assessments, the established policies and procedures were not being followed. He stated that NNSA will provide a copy of our recommendations and NNSA's expectations to the Site Office Managers for their inclusion in their respective oversight processes.

Regarding recommendation 2, the Associate Administrator stated that the contracting officer already determined that the costs incurred to change the locks are allowable and reasonable under the terms of the contract, and NNSA did not believe that the matter requires an "Allowability of Cost Determination." However, he advised that NNSA is requesting a General Counsel opinion as to what warrants an "Allowability of Cost Determination." In addition, the Associate Administrator did not believe the $1.7 million figure stated in our draft report to replace or upgrade

approximately 100,000 locks was consistent with the Laboratory's expenditures or number of locks being replaced. The Associate Administrator did not provide figures for the actual cost and numbers of locks to be replaced. In addition, as of the date of this report, NNSA has not provided these figures.

Regarding recommendations 3, 4, 5, and 6, the Associate Administrator identified ongoing and completed corrective actions taken by the Livermore Site Office and Laboratory management that he felt were responsive to our recommendations.

The complete text of management's comments are attached at Appendix B.

INSPECTOR COMMENTS

Management's actions appear responsive to the report recommendations. However, we do not agree that the total cost of replacing and upgrading the locks are "part of the normal cost of doing business." Livermore did not follow its internal procedures for the control and accountability of master keys and master Tesa cards, which created a security vulnerability that resulted in the need to replace and upgrade a significant number of locks. By not complying with its contractual responsibilities, the Laboratory unnecessarily incurred a substantial cost that we believe is unallowable and should not be borne by the taxpayer.

Management identified actions implemented by the Livermore Site Office and the Laboratory to ensure proper reporting of incidents such as the missing master keys and master Tesa cards. These actions included implementation of additional procedures and training. We believe these actions are a good first step to address the problems discussed in our report. However, as acknowledged by the Associate Administrator, in specific instances established processes and procedures were not followed. Therefore, in addition to issuing additional procedures, we believe management should assure that a culture exists wherein individuals will fully implement the procedures.

Appendix A

SCOPE AND METHODOLOGY

The fieldwork for this inspection was conducted between May and July 2003. We interviewed numerous Livermore and NNSA Livermore Site Office officials regarding their knowledge of the missing master keys and master Tesa cards. We also reviewed available documentation from the Livermore internal and external review teams that evaluated the missing master key and master Tesa card incidents. The documentation that we reviewed included:

- Incident Assessment Team Report: Key Incident of April 17, 2003.
- Independent External Review Team "Report on the Lawrence Livermore National Laboratory Security Key Incident."
- Incident Analysis Team Report dated May 30, 2003.
- Master Tesa Inventory Process Report (Revision 1), dated June 6, 2003.
- Lawrence Livermore National Laboratory "Locks and Keys Guide."
- Fiscal Year 2003 Appendix F, Performance Assessment Mid-Year Review.
- Integrated Safeguards and Security Management Project Plan, dated December 14, 2001.
- LLNL Implementation Guidelines for Fiscal Year 2003 Appendix F Performance Objectives and Measures.

We also reviewed the contract between DOE and the University of California for the management and operation of Lawrence Livermore National Laboratory, as well as:

- DOE Notice 471.3, "Reporting Incidents of Security Concern."
- DOE Notice 473.8, "Security Conditions."

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Appendix B

National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

OCT 1 0 2003

MEMORANDUM FOR Alfred K. Walter
Acting Assistant Inspector General
for Inspections and Special Inquiries

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Draft Report on LLNL Security Incidents

NNSA appreciates the opportunity to review the Inspector General's (IG) draft Inspection report, "Reporting of Security Incidents at the Lawrence Livermore National Laboratory." We understand that the objectives of the inspection were to determine: (1) the adequacy of internal controls at Livermore over the timely and appropriate reporting of security incidents such as the missing master keys and master TESA cards, and the identification and correction of corresponding potential security vulnerabilities; and, (2) if performance measures exist at Livermore that adequately address the reporting of such incidents.

We appreciate the IG's efforts and believe that the report is consistent with the findings of the Laboratory, Livermore Site Office, University of California, and NNSA conducted reviews of the security locks and keys incidents. While the report only explores the chronology and activities of the missing master keys and master TESA cards, NNSA believes that the report should acknowledge that formal corrective action plans, to correct vulnerabilities in security incident reporting and security key control and inventory, were prepared by the Laboratory, approved by the Site Office, and were already in place in July 2003. In fact, there were three major findings related to security locks and keys issued by the Site Office to the Laboratory on June 12. The Laboratory subsequently submitted the corrective action plans, with a detailed project schedule, for each of the findings to the Site Office. We believe it is important to mention that there are several corrective action milestones that have been achieved and will have been validated by the Site Office by the end of December.

The report has a recommendation related to the determination as to whether the costs associated with the corrective actions are reasonable and allowable. NNSA's position is that the costs are reasonable and allowable. However, we

Printed with soy ink on recycled paper

realize the intent of the recommendation and by copy of this response, NNSA is requesting a General Counsel opinion as to what warrants an "Allowability of Cost Determination." An "Allowability of Cost Determination" is a formal contract process utilized by Contracting Officers when there are questionable costs associated with a contract. We do not believe that this issue falls into that category. However, as stated, we look forward to the opinion of our General Counsel.

NNSA's specific comments related to the recommendations are as follows:

1. For the Administrator to "Ensure that field site security surveys and self-assessments include a review of internal controls relating to the issuance, receipt, and inventory of all keys involving sensitive areas."

NNSA believes that the processes are in place related to security of keys and are captured in the surveys and self-assessments. We further believe the established processes and procedures were not followed. NNSA will provide a copy of the recommendations and NNSA's expectations to the Site Office Managers for their inclusion into their respective oversight processes.

2. Review the costs incurred by Livermore to replace and upgrade approximately 100,000 locks necessitated by the missing master keys and master TESA cards, to determine whether the costs are reasonable and allowable.

While NNSA does not believe that this issue requires an "Allowability of Cost Determination," the contracting officer already determined that the costs incurred to change locks are allowable and reasonable under the terms of the contract. When keys are discovered missing that can create a potentially adverse security situation, it is incumbent upon the Laboratory to take appropriate action.

The $1.7 million stated in the report to replace or upgrade approximately 100,000 locks is not consistent with the Laboratory's expenditures or the number of locks being replaced. The resources committed to the corrective actions have come from existing program funding and include equipment upgrades made at the request of LLNL Programs. Installation of TESA electronic locks to replace mechanical keys/cores offers better modernized security and has been an ongoing process over the past five years. Replacing missing keys and TESA locks are considered part of the normal cost of doing business.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

3. Ensure that Livermore establishes appropriate internal controls to correctly identify reportable incidents, and that such incidents are reported in a timely manner.

Incident reports are distributed daily to appropriate personnel via fax to the Incidents and Infractions Section, Office of Investigative Services (OIS), Physical Security Group, and to the Site Office. The Laboratory has put in place procedures for classification review, risk assessment and dissemination of Protective Force Division (PFD) incident reports. Procedural documents: "LLNL Implementation Procedures for Reporting Incidents of Security Concern"; "Security Duty Officer Reporting Procedures"; "PFD Incident Report Review"; and, "Reporting Incidents of Security Concern" were submitted to the Site Office on September 30.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

4. Ensure that Livermore officials responsible for categorizing incidents reportable under DOE Notice 471.3 are trained to properly determine the appropriate IMI classification level of security incidents.

The Security Incident Reporting Officer and the Safeguards and Security Deputy Manager have received updated training provided by DOE/NNSA Headquarters in August.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

5. Ensure that internal controls are established by Livermore that promote the timely assessment of vulnerabilities resulting from security incidents and the prompt implementation of compensatory measures.

The Laboratory implemented and submitted a procedural document titled, "Security Duty Officer Reporting Procedures" on September 30, to the Site Office, to address vulnerabilities and implementation of compensatory measures.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

6. Ensure that Livermore has established appropriate internal controls for the management and inventory of master keys and master TESA cards.

The Laboratory has completed a 100 percent inventory and reconciliation of all grand master keys. Results of the inventory are written in a report titled, "Status of Master Security and 'Z' Key Inventory Process" dated July 25, 2003. Additionally, accountability and inventory requirements are written in each of the following documents: "Locks and Keys Policy" dated September 17, 2003; "Locks and Keys User Manual", dated September 30, 2003; and, "Locks and Keys Procedures" dated September 30, 2003.

NNSA believes that the actions taken by the Site Office and the Laboratory are responsive to the recommendation and are complete.

cc: NNSA General Counsel, NA-3.1
Edward J. Knuckles, Assistant Manager-Business, Livermore Site Office
Robert Braden, Senior Procurement Executive, NA-63
David Marks, Field CFO, SvcCen/NV

IG Report No. DOE/IG-0625

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

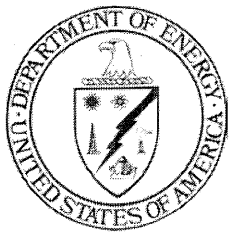
If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

10



U.S. Department of Energy
Office of Inspector General

Special Report

Management Challenges at the Department of Energy

DOE/IG-0626

November 2003

Department of Energy

Washington, DC 20585

November 12, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Report on "Management Challenges at the Department of Energy"

BACKGROUND

For the past several years, the Office of Inspector General has identified what it considers to be the most significant management and performance challenges facing the Department of Energy. This effort, now codified as part of the Reports Consolidation Act of 2000, is completed on an annual basis, reflecting new work performed by the Office of Inspector General, an assessment of the agency's progress in addressing previously identified challenges, as well as emerging issues facing the Department. This year we have used a different methodology for categorizing the challenges, essentially distinguishing between mission-related areas with inherent management risks and those aspects of the Department's operations in which we have identified specific internal control challenges. Additionally, we have developed a "watch list" that reflects operational or programmatic functions that need, in our judgment, to be closely monitored by Department management.

RESULTS

Based on work performed by the Office of Inspector General in the past year and on other relevant information, the following are the most serious challenges facing the Department of Energy:

Mission-Related Challenges	Internal Control Challenges
• Environmental Cleanup	• Contract Administration
• National Security	• Project Management
• Stockpile Stewardship	• Information Technology

Each of these challenge areas has been a long-standing and widely acknowledged issue for the Department. The mission-related challenges reflect inherent operational risks, which, in many cases, involve actions beyond the Department's direct control. These are likely to continue into the future.

Beginning in March of 2003, senior Department leadership, at your direction, initiated a robust initiative to address – and, if possible, resolve – each of the management challenges identified in our previous report, *Management Challenges at the Department*

Printed with soy ink on recycled paper

of Energy (DOE/IG-0580, December 2002). The Deputy Secretary, as the leader of this initiative, has been personally invested in its operation, working with the Under Secretaries and Assistant Secretaries to achieve progress. Based on our analysis of this effort, if this initiative continues with the personal involvement of the Department's senior leadership, the processes for defining challenge areas, identifying root causes, and establishing effective corrective action plans will be measurably improved. In fact, during our review, we concluded that sufficient progress was made in two areas reported as challenges last year – performance management and worker and community safety – that we have moved them to our watch list. This list can be found in Appendix 1 of this report.

Also, on this year's watch list, we have included disruptions in energy supply as an emerging issue. One of the primary reasons for the creation of the Department was the need for a coordinated national response to the economic and social turbulence caused by the oil embargo that occurred during the 1970s. Given our continued reliance on foreign sources of energy, recent major disruptions to our energy supply, and the resulting questions concerning the status of our energy infrastructure, it is clear that this will be a major component of the Department's agenda into the future.

It should be noted that the Department, in its Fiscal Year 2003 Performance and Accountability Report, identifies a similar set of issues that impact the Department's ability to fulfill its critical missions. In this regard, the Office of Inspector General will work closely with Department officials to evaluate agency performance in an effort to improve programs and operations, particularly as they relate to the management challenge areas identified in this report.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science and Environment
Administrator, National Nuclear Security Administration
Director, Office of Management, Budget and Evaluation/Chief Financial Officer
Chief of Staff

MANAGEMENT CHALLENGES AT THE DEPARTMENT OF ENERGY

TABLE OF CONTENTS

Analysis of Management Challenges

Background 1

Mission Related Challenges 1

Internal Control Challenges 6

Appendices

1. Watch List 13

2. Table Comparing Management Challenges Reported by Various Groups 15

3. Related Reports Issued in Fiscal Year 2003 16

ANALYSIS OF MANAGEMENT CHALLENGES

Background

The Department of Energy (Department) is engaged in work vital to our nation's security and economic growth. Its missions address a wide range of areas including science, energy resources, national nuclear security, and environmental quality. To accomplish these missions, the Department receives annual appropriations of about $21 billion, employing about 15,000 Federal and 100,000 contractor personnel and managing more than $110 billion of assets.

As required by the Reports Consolidation Act of 2000, this report documents the Office of Inspector General's judgment as to the most serious management challenges facing the Department. We have categorized the six challenges identified as either mission-related or internal control. Our conclusions are drawn primarily from our audits, inspections and investigations of the Department and its operations, but also consider other sources of data.

Mission Related Challenges

Certain management challenges deal with long-standing mission related risks that are inherent to the Department's complex operations. These challenges are likely to persist well into the future, in part, because they involve factors that are outside of the Department's direct control. We concluded that the Department faces three such challenges: Environmental Cleanup, National Security, and Stockpile Stewardship.

Environmental Cleanup

The Department's program for cleaning up the environmental contamination caused by nuclear weapons research, production, and testing is the Department's single largest financial liability – estimated to cost about $210 billion over the next several decades. Environmental cleanup activities include many complex technical and regulatory challenges. In fact, some of the Department's disposal facilities are unique in the world. Moreover, the Department operates in a regulatory environment governed by complex Federal statutes, approximately 70 compliance agreements with states and other Federal agencies, and over 7,000 enforceable milestones. While the Department has made great strides in addressing the inherent risks in this area, it has not consistently met its goals or integrated its programs for site cleanup and waste disposal.

In our report on *Waste Reduction Plans for the Advanced Mixed Waste Treatment Project at the Idaho National Engineering and Environmental Laboratory* (DOE/IG-0611, July 2003), we concluded that the project will only reduce waste volume at Idaho by 6 percent,

instead of the planned 65 percent. As a result, the Department may spend $250 million more than expected to dispose of this waste. As another example of cleanup goals unmet, in our report on *Disposal of the Rocky Flats Environmental Technology Site's Low-Level Mixed Waste* (DOE/IG-0612, July 2003), we noted that, due to regulatory difficulties in permitting a waste disposal site to accept waste, the Department is at risk of missing closure targets and incurring significant cost increases in order to deal with certain types of waste at Rocky Flats.

The Department has also faced difficulties in integrating its cleanup efforts. For example, our report on *The Department of Energy's Spent Nuclear Fuel Canisters and Transportation Casks*, (DOE/IG-0608, June 2003) found redundancies in the development of canisters and transportation casks between Department sites. In another report, *Treatment of Mixed Incinerable Waste* (DOE/IG-0588, March 2003), we noted inefficiencies in the treatment and storage of this waste at several sites. Specifically, although a Department-owned incinerator was used at less than one-third of its capacity, and another treatment system was used at just over half capacity, the Department was funding a treatment facility owned by a commercial vendor that may duplicate the Department's underutilized facilities. Further, our report on *Disposal of Remote-Handled Transuranic Waste at the Waste Isolation Pilot Plant* (DOE/IG-0613, July 2003) disclosed significant inconsistencies between the waste-generating site plans and the Departmental plan for treatment and disposal of remote-handled transuranic waste.

To correct the issues raised in our reports, the Department's Office of Environmental Management has initiated a number of specific actions. Also, in March 2003, at the Deputy Secretary's request, the Assistant Secretary for Environmental Management initiated a number of actions intended to help the Department deal more effectively with cleanup activities and to accelerate reforms recommended in Environmental Management's 2002 "Top to Bottom" review. These actions included:

- Developing and implementing a new budget structure;
- Instituting human capital reforms;
- Modifying the acquisition strategy by using more small, discrete cleanup contracts;
- Organizing a management advisory council to review contracts from a corporate perspective, and to find ways to improve performance of contractors;

- Enhancing configuration control over critical program elements, including corporate performance metrics, contractor performance measures, and life-cycle costs; and,
- Pursuing innovative solutions to cleanup through the creation of ten integrated project teams.

The Office of Inspector General will continue to allocate its resources to assist the Department in this critically important area.

National Security

The Department plays a key role in the Nation's national security apparatus, including major programs related to the non-proliferation of nuclear weapons and a number of programs that are relevant to homeland security. Since September 11, 2001, the Department's activities in this area have been operating in an increasingly dynamic and challenging world. Our reviews have highlighted areas that need attention to strengthen the Department's efforts in domestic threat response and protection, nonproliferation, site access controls, and protective forces.

The Department plays a critical role in protection of the domestic infrastructure. Through our reviews, we have identified areas that need enhancement. Our review of *National Nuclear Security Administration's Ability to Meet the Aircraft Requirements of the Joint Technical Operations Team* (DOE/IG-0605, June 2003) found that the National Nuclear Security Administration (NNSA) was not prepared to meet the requirements of the Joint Technical Operations Team, which was established to respond to terrorist attacks involving nuclear weapons. Also, the Department did not have formal agreements with the Department of Defense to detail specific requirements to support this critical mission. In another report, which is not publicly releasable in its entirety because it contains information that is Official Use Only, *Actions Taken in Response to Missing Hazardous Waste Containing Cyanide* (DOE/IG-0592, March 2003), we noted that the Department needs to enhance awareness of materials that could be used as weapons of mass destruction and to strengthen controls over management and disposition of these materials. Further, in our report, *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003), we concluded that two power administrations did not adequately assess vulnerabilities or risks for their most critical assets. As a result, these power distribution assets could be more vulnerable to attack, which could lead to economic impacts on the power administrations and their customers.

Related to international nonproliferation issues, the Office of Inspector General issued a report on *International Materials Protection, Control and Accountability Non-Proliferation Initiative* (DOE/IG-0603, June 2003), in which we concluded that a significant portion of funding was expended in the United States, rather than being used directly to reduce proliferation risks in the former Soviet Union. In fact, the Department's national laboratories spent a combined total of $13.7 million more than Congressional targets for domestic expenditures in Fiscal Year (FY) 2001 and FY 2002. Also, the Department allowed uncommitted funds to increase to $133 million by the end of FY 2002. Our report also noted that improvements were needed in prioritizing and allocating funds, and measuring performance.

As in previous years, the Office of Inspector General issued several reports regarding access controls over Departmental operations. For example, our report on *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 2002) disclosed that the Department had not adequately controlled unclassified visits and assignments by foreign nationals. Also, in our report on *Personnel Security Clearances and Badge Access Controls at Selected Field Locations* (DOE/IG-0582, January 2003), we identified significant discrepancies at Oak Ridge where the Department had either not terminated former Federal and contractor employees' clearances or had not recovered their badges. Less significant but related problems were identified at other sites during this review.

The Department of Energy and its contractors are also responsible for producing, storing, and handling significant quantities of nuclear materials, weapons, and other national security related information. Through its contractors, the Department employs protective force personnel as key elements in the protection of its facilities. During the review of *Management of the Department's Protective Forces* (DOE/IG-0602, June 2003), the Office of Inspector General concluded that several significant weaknesses existed, including: long delays in granting clearance to protective force personnel; increases in unscheduled overtime cost; morale and retention problems because of mandatory overtime; and, operational vulnerabilities with work stoppages. Another review concerning the readiness of the Department's protective forces, *Inspection of Implementation of Corrective Actions Resulting From Force-on-Force Performance Tests* (DOE/IG-0585, February 2003), determined that the process of documenting activities associated with corrective action plan milestones at Los Alamos could be improved. Also, we noted areas where internal policies and procedures at Pantex could be strengthened in order to improve readiness of the Department's protective forces.

Recently, the Department has taken several steps to improve security controls and mitigate associated risks. For instance, in March 2003, the Department issued its strategic plan for security, outlining its priorities, goals, initiatives, and challenges for the next decade. Additionally, as part of the Deputy Secretary's effort to address management challenges, the Department conducted an assessment of its security posture and concluded that three major areas of risk exist: the evolution of new and emerging threats; problems with prioritizing and assigning scarce resources; and, unclear assignment of accountability, roles and responsibilities. Senior Departmental management, including the Under Secretary for Energy, Science and Environment, the Administrator for NNSA, and the Office of Security have initiated actions intended to improve performance in these areas. Additionally, the Department has a Security Policy Streamlining Initiative and has formulated an Executive Quality Panel to improve the Department's policies and procedures over security.

Stockpile Stewardship

The Department's program for stockpile stewardship is one of the most technically complex scientific programs ever undertaken. Specifically, the Department is charged with maintaining the safety, reliability, and performance of the nation's nuclear weapons stockpile in the absence of underground nuclear testing. The Secretary of Energy must annually certify to the President that the weapons are safe and reliable and that underground testing does not need to be resumed. To accomplish its mission, the NNSA is developing a remarkable set of scientific facilities and tools to (1) better understand changes that occur in nuclear weapons as they age, (2) enhance stockpile surveillance capabilities, and (3) extend the life of weapons in the stockpile. In meeting these challenges the Department has had difficulty with the efficiency of its operations, administrative processes, and the ability to conduct timely studies of weapons systems.

A review of *Beryllium Oxide Operations at the Y-12 National Security Complex* (DOE/IG-0595, April 2003) disclosed that there were inefficiencies in Y-12's beryllium oxide operations. For example, operations were spread out across the Y-12 site, and equipment and facilities were outdated. Additionally, the Department did not adequately consider using other materials that would perform the same function as beryllium but without the harmful health effects. Another report, *Management of Beryllium Metal Supply* (DOE/IG-0583, January 2003), noted that only 50 tons of beryllium in the National Defense Stockpile is reserved for the Department, yet there is a need for 90 tons of beryllium over the next three decades. We made recommendations

intended to help the Department close this potential gap. In a different case, our report on *Reconfiguration of the Kansas City Plant* (DOE/IG-0616, August 2003) found that the Stockpile Management Restructuring Initiative will not achieve the goals established in the initiative, and, consequently, will not save as much money as anticipated.

Some of NNSA's administrative processes need strengthening as well. In our report on the *National Nuclear Security Administration's Planning, Programming, Budgeting and Evaluation Process* (DOE/IG-0614, August 2003), we found that while NNSA had made significant progress toward the implementation of its PPBE process, several areas needed to be addressed before the process is fully operational. Specifically, NNSA managers were not always clear on their roles and responsibilities; contractor estimates that form the basis for budget estimates were not validated; and, an independent analysis group to support the resource allocation decision process had not been established.

In addition, delays that could put stockpile stewardship program goals at risk were identified in our report on the *National Nuclear Security Administration's Nuclear Explosive Safety Study Program* (DOE/IG-0581, January 2003), which found that Nuclear Explosive Safety studies were delayed for six of the nine nuclear weapon types. These delays would cause an actual time difference between the comprehensive studies of 11 to 16 years, exceeding the standard of every ten years.

To its credit, as part of the Deputy Secretary's effort to mitigate risks associated with management challenges, NNSA management has initiated corrective actions intended to address these concerns. Initiatives are underway to improve management processes over planning and budgeting, information management, acquisitions, and human resources.

Internal Control Challenges

Internal control challenges represent issues that, if not addressed, may impede the Department's ability to carry out its program responsibilities and to ensure the integrity of its operations. These challenges relate to the Department's management processes for achieving its mission rather than directly to the mission outcomes themselves. We concluded that the department faces three challenges related to internal control systems: Contract Administration, Project Management, and Information Technology.

Contract Administration

Most of the Department's operations are carried out through contracts that consume about seventy five percent of the Department's $21.3 billion budget. Contracts and grants are awarded to industrial companies, academic institutions, and nonprofit organizations that operate a broad range of scientific, industrial, and production facilities. The Department has traditionally faced challenges with contract administration, and the Office of Inspector General continues to consider it a management challenge. The National Aeronautics and Space Administration (NASA) has recently been criticized for its "hands-off" approach to contracting in conjunction with space shuttle operations. For example, in January 2003, the General Accounting Office issued a report that cited NASA's lack of effective contract oversight activities. Like NASA, contracting out is a key element of the Department of Energy's management culture. As a consequence, Federal managers need to avoid becoming too insulated from program performance. Clearly, the issues discussed in this management challenge transcend the functional role of procurement. Other administrative areas such as program and financial management influence the effectiveness of the Department's contract administration. Our reviews identified the need for improvement in the oversight of the following areas: contract cost, laboratory and community development activities, and grants to local governments.

Inadequate oversight of costs of contracts has been a long-standing management issue for the Department. In our report on *The Advanced Mixed Waste Treatment Facility Contract at the Idaho National Engineering and Environmental Laboratory* (DOE/IG-0622, September 2003), we concluded that the Department is paying for equipment and services that are no longer being contemplated in the project. The report identified an opportunity for the Department to reduce the contract by more than $90 million. Additionally, Office of Inspector General reviews have disclosed instances where costs were incurred and paid by the Department that we consider to be questionable. For example, in our report on the *University of California's Costs Claimed and Related Internal Controls for Operation of Los Alamos National Laboratory* (DOE/IG-0596, April 2003), we identified potentially unallowable costs of about $14.6 million that were charged to the contract for "working" meals, travel costs in excess of contract limits, and for an internal audit function that did not meet Departmental requirements. Further, in our special inquiry report on *Operations at Los Alamos National Laboratory* (DOE/IG-0584, January 2003), we described actions taken by Laboratory officials that weakened or

overrode property and procurement management controls. In addition, this report identified practices by management that may have discouraged employees from raising concerns to appropriate authorities. Contractor employees should feel free to disclose concerns about contract operations to appropriate parties without fear of retaliation.

The Department allows contractors to engage in certain business development activities to facilitate the prospect of acquiring new sources of revenue for laboratories. Work conducted by the Office of Inspector General indicates that the Department needs to improve its administration of these activities. In the report on *Idaho National Engineering and Environmental Laboratory's Strategic Initiative Fund*, (DOE/IG-0601, May 2003), we noted that the Department's oversight of a mission development fund at Idaho was insufficient. Specifically, we identified instances where the fund may have been used to supplement other restricted funds and to pay for activities that could have been funded directly.

Additionally, we performed a review dealing with the Department's involvement with local economic development groups. Our report on *Utility System Leases at the East Tennessee Technology Park* (DOE/IG-0609, June 2003) disclosed that the Department did not obtain competitive bids for management of the utility systems and infrastructure. Also, we questioned $6.9 million in costs. Similarly, in *Transfer of Excess Personal Property from the Nevada Test Site to the Community Reuse Organization* (DOE/IG-0589, March 2003), our report disclosed that Nevada's property transfer practices to community reuse organizations did not strike an appropriate balance between the effort to assist community development and the need to ensure that taxpayers received reasonable consideration for property transferred. For example, a drill rig potentially worth $3.9 million was sold to the community re-use organization for $50,000.

In addition, under terms of the Nuclear Waste Policy Act, the Department provides funds to the State of Nevada and several local governments to oversee the Department's Yucca Mountain Project. Our report, *Oversight Funds Provided to Local Governments in the State of Nevada* (DOE/IG-0600, May 2003), disclosed that three counties used oversight funds for activities that were prohibited by the Nuclear Waste Policy Act, such as hiring a lobbyist and sponsoring rallies to protest the Yucca project. In a similar review, *Inspection of Savannah River Operations Office Management of Emergency Response and Law Enforcement-Related Grants* (DOE/IG-0604, June 2003), we concluded that the Department was not adequately managing grants to Georgia and South Carolina and did not have documentation to support whether or not the grant recipients were on schedule and meeting milestones.

The Department's Chief Financial Officer, at the request of the Deputy Secretary, has developed a corrective action plan to address five major areas of contract administration in which improvement is desired: selection of contract type; increasing competition; use of effective performance objectives and measures in contracts; effective management of Departmental initiatives; and, inadequate human resources to perform contract oversight. The Chief Financial Officer has identified specific actions for each of these major areas that are intended to improve the Department's performance in contract administration. Notably, the Department is taking steps to compete the Los Alamos National Laboratory contract for the first time in 60 years.

Project Management

In carrying out its various missions, the Department is engaged in numerous multi-million dollar – and a few multi-billion dollar – projects. Because of the scientific and technologically complex nature of much of the Department's work, many of the projects are unique in the world. For many years, however, the Department has been criticized for weaknesses in its project management. In an effort to delineate and address those weaknesses, the Department has, since 1998, engaged the National Research Council (an organization of the National Academies of Science) to make recommendations to improve project management. The Council published a series of reports, which concluded that the Department lacks sufficient control over its projects, ultimately resulting in projects with cost and schedule over-runs. In its most recent report, Progress in Improving Project Management at DOE – 2002 Assessment, the Council expressed concern over the Department's consistency and continuity of applying project management principles, risk management, and contingency. The Council cited improvements in the Department's organizational structure with a central project management office, improved policies and procedures over project management, improved project management tools, and improvement over human resource issues pertaining to project management. Through these efforts, the Department has improved management of traditional construction projects. In our judgment, these same concepts should also be applied to the Department's operating projects.

In our work related to environmental cleanup projects, the Office of Inspector General reported on instances in which the Department had not appropriately applied project management principles, including thoroughly analyzing the cost-effectiveness of proposed new facilities. For example, our report on *Planned Characterization Capability at the*

Waste Isolation Pilot Plant (DOE/IG-0577, December 2002), disclosed that a proposed central characterization facility for transuranic waste at the Waste Isolation Pilot Plant would not benefit generator sites and may not be needed. Also, our report on the *Idaho National Engineering and Environmental Laboratory's Remote Treatment Facility* (DOE/IG-0573, November 2002) found that the conceptual plan for the planned facility did not provide the capability to treat all remote-handled solid waste at the Idaho site. Further, in a report on the *Idaho Settlement Agreement Activities* (DOE/IG-0571, October 2002), we noted that two recently completed cleanup projects overran costs by a combined $168 million. In this report, we made recommendations to improve project controls over operating projects.

In the stockpile stewardship area, our review of the *Dual Axis Radiographic Hydrodynamic Test Facility* (DOE/ IG-0599, May 2003) disclosed that this facility would not be operational until June 2004, 15 months behind schedule, even after scope changes that reduced or eliminated work elements. Additionally, in our report on *Refurbishment of the W80—Weapon Type* (DOE/IG-0590, March 2003), we found it to be unlikely that NNSA's W80 refurbishment projects will meet scope, schedule, and cost milestones. Lawrence Livermore and Sandia National Laboratories cancelled or delayed testing without notifying NNSA or updating the project plan. We made recommendations to improve the accountability and oversight over this project.

Also, in our review of *Plutonium-238 Production* (DOE/IG-0607, June 2003), we concluded that there were risks that the Department would not achieve its plutonium 238 production objectives. We recommended the Department implement project management controls over the project, better define long-term needs, and designate the project as a high priority.

To address project management issues identified by the National Research Council, the Office of Inspector General, and other reviewers, the Department's leadership has initiated a number of corrective actions, particularly for capital asset construction projects. Examples include using External Independent Reviews to ensure quality planning during early stages of the projects; regular status reports with senior Department management; conducting executive level management reviews; and, implementing a new career development program for project managers. Additionally, some Departmental organizations, such as the Office of Environmental Management, are reforming the way its projects are organized and administered in order to improve accountability and effectiveness.

Information Technology

The Department spends more than $2 billion annually on information technology resources. In the past year, a number of Office of Inspector General reports have highlighted internal control weaknesses that impact cyber security and the improvement of information technology systems.

Our report on *Remote Access to Unclassified Information Systems* (DOE/IG-0568, September 2002) disclosed that the majority of offices reviewed had not adequately protected information systems from unauthorized remote access. This placed them at risk for tampering, fraud, and other criminal acts. In our report *Security Over Wireless Networking Technologies* (DOE/IG-0617, August 2003), we reported that four of the six organizations we reviewed had deployed wireless networks without assessing the risks associated with their use. This placed the Department's information systems at risk of attack from internal and external sources and could ultimately result in the compromise of critical systems and information.

Also, in our evaluation report on *The Department's Unclassified Cyber Security Program 2003* (DOE/IG-0620, September 2003), we noted a number of improvements in the Department's unclassified cyber security program since our last review; however, we observed that problems continue to exist in several critical areas. In an interim report *on Inspection of Internal Controls Over Personal Computers at Los Alamos National Laboratory* (DOE/IG-0597, April 2003), we found that the controls over classified and unclassified laptop computers were inadequate. Los Alamos could not account for its single-user classified laptops. Further, computers that could not be located were simply written off without sufficient review of the circumstances, and thefts were not always reported to the Laboratory's Office of Security Inquiries.

To its credit, the Department's Office of Chief Information Officer is developing corrective actions to mitigate cyber-security risks and to improve relevant controls. For instance, the Department is finalizing detailed cyber security policy and guidance, and in June 2003 provided guidance for cyber-security performance measurements. Additionally, the Department recently issued DOE Order 205.1, Department of Energy Cyber Management Program, which requires that continuity of operations, configuration management, and incident reporting procedures be developed and maintained in Program Cyber Security Plans and Cyber Security Program Plans. Additionally, the Office of

the Chief Information Officer has addressed inadequate reporting in its draft Incident Prevention, Warning, and Response manual. Specifically, the draft includes guidance on reporting to law enforcement and the Office of Counterintelligence. Moreover, the draft manual addresses the lack of reporting by requiring monthly verification when no reportable incidents occur.

For some time, the Department has experienced problems in fully implementing the requirements of the Clinger-Cohen Act of 1996. These requirements established the Department's Chief Information Officer, who was to have broad authority to use information technology to improve performance and reduce costs. The Department has identified significant barriers to achieving Clinger-Cohen's objectives, including: the decentralized approach to information technology management in the Department; the Chief Information Officer's limited role in the budgeting process for Departmental programs; and, the lack of a baseline of information technology to guide the acquisition and management of information technology resources in the Department.

In our report on *Information System Development Practices at the Bonneville and Western Area Power Administrations* (DOE/IG-0586, February 2003), the Office of Inspector General found that system development was not always consistent with Federal requirements and guidance. The absence of key system development activities led to schedule slippage and a $9 million write-off. Also, Bonneville faced development delays of more than two years and modifications costing more than $600,000. Further, three different regional offices had separate billing systems for the same core purpose. In another report, *Business Management Information System* (DOE/IG-0572, November 2002), we concluded that the system under development was unlikely to satisfy some key Federal requirements and was not aligned with the Department's corporate information technology architecture. Specifically, program elements were developing separate systems that were not capable of full integration with other business systems; did not link performance and financial data; and, did not replace inefficient program and site-level financial management systems.

To better delineate its policies and procedures on information technology issues, the Department is preparing a DOE Order on information technology management. Also, the Chief Information Officer is developing an acquisition framework and an information technology investment portfolio system to improve decision making for new information technology acquisitions, and to improve information technology capital planning. Further, the Department plans to complete an information technology enterprise architecture-based information technology inventory.

Appendix 1

WATCH LIST

The Office of Inspector General's "watch list" consists of management issues that do not, in our judgment, meet the threshold of major management challenges yet warrant continued attention by senior Department managers. Watch list issues may include management challenges identified in previous years for which the Department has implemented corrective actions or has achieved positive outcomes. The watch list may also include emerging issues that may require Department action. This year's watch list addresses three areas: Energy Supply; Worker and Community Safety; and, Performance Management.

Energy Supply

One of the Department's strategic goals is to promote the development and deployment of energy systems that will provide the Nation with clean, efficient, economical and reliable energy. This strategic goal recognizes the critical role energy contributes to the Nation's economy and to our standard of living. In fact, one of the primary reasons the Department of Energy was created in 1978 was the need for a coordinated national response to the economic and social turbulence caused by energy supply disruptions that occurred in the 1970s, such as the Oil Producing and Exporting Countries oil embargo of 1973 and 1974. Disruptions in energy supply can cause dramatic price fluctuations that reverberate throughout the Nation's economy.

Nevertheless, for the past several decades, the United States has been increasingly dependent on energy supplied by foreign sources, especially petroleum imports from the Persian Gulf region. From 1981 to 2001, the percent of United States petroleum needs met from foreign sources increased from 34 percent to 54 percent and is likely to continue to increase further in the future. Acknowledging the trend toward increasing dependence on foreign energy sources, the President's FY 2004 budget proposal for the Department of Energy identifies "reduce dependence on energy imports" as one of the Department's six primary priorities.

It is important to note that risks of disruptions in energy supply are not restricted to foreign oil imports. Other recent events indicate that challenges exist in many areas of energy supply. For example, in August 2003, more than 20 million people in the northeast were without electricity during the largest blackout in U.S. history. Further, in the summer of 2001, large areas of the State of California were subjected to rolling blackouts. Also, acute shortages of natural gas resulted in dramatic price increases in 2003, and spikes in the price of gasoline have occurred for a myriad of reasons including domestic pipeline issues. Aging nuclear facilities also continue to play a significant role in domestic power generation. Accordingly, it appears that the risks of energy supply disruptions will be on the Department's agenda for the foreseeable future. Given our reliance on energy, this will be one of the most important policy decisions facing the nation. As the Federal agency responsible for energy policy at the national level, the Department will have a critical role in addressing this challenge.

Worker and Community Safety

The Department manages large amounts of dangerous materials and operates large-scale industrial facilities that represent safety risks to workers and local communities. Safety incidents that affect workers and the community have the potential to destabilize, delay, and disrupt the Department's critical activities, and have intangible costs such as a negative public perception of the Department. Accordingly, it is imperative that the Department continue to place a high priority on worker and community safety. In prior years, we reported worker and community safety as a major management challenge.

This year, due to progress made and actions currently underway, we moved this area to our watch list. Specifically, the Department has implemented an improvement action plan that details 26 commitments. For example, the Department has improved definition and assignment of organizational roles, responsibilities, and authority. Also, the Department has implemented processes to improve safety analyses and design codes.

The Office of Inspector General continues to evaluate the Department's safety programs and activities and to make recommendations to assist management in improving its operations. For example, our report on *Inspection of Explosives Safety at Selected Department of Energy Sites* (DOE/IG-0578, December 2002) noted that improvements could be made in the areas of explosives safety, fire, and lightning safety.

Performance Management

In previous years, we have reported that performance management was among the most serious challenges the Department faced. Specifically, we noted that:

- Performance measures were frequently not clear or quantifiable;
- Some major Departmental activities lacked performance measures; and,
- Reported performance results were not always accurate and valid.

We have concluded, however, that in the past year, the Department has made considerable progress in addressing these concerns. The Department's Office of Chief Financial Officer led the Department's efforts to improve performance management. These efforts, coupled with the Deputy Secretary's initiatives to establish program office "ownership" of Department challenge areas and to develop corrective action plans for each are positive steps. In our judgment, senior Department leadership has acted forcefully to establish meaningful performance management improvements. Actions implemented to date include: issuing new policy on performance measures to better define terminology and criteria; rolling out a new performance measurement software system that forces performance data to be quantifiable; conducting new training on performance measurement; and, implementing an Earned Value Management System on projects with funds of $5 million or more. Nevertheless, many of the improvements in this area are new and require the continued diligent attention of senior Department management to assure accurate and valid results are reported and documented against clear and meaningful measures.

Appendix 2

TABLE COMPARING MANAGEMENT CHALLENGES REPORTED BY VARIOUS GROUPS

IG	GAO[1]	DOE[2]
Contract Administration	Contract Management	Program Oversight of Contractors
Environmental Cleanup	Cleanup of Radioactive & Hazardous Waste	Environmental Cleanup
		Nuclear Waste Disposal
Information Technology Management		Information Technology Management
National Security	Security Threats and Problems	Security
		Performance Management
Stockpile Stewardship	Nuclear Weapons Stockpile	Stockpile Stewardship and Testing
		Safety and Health
		Human Capital Management
	Revitalize Infrastructure	Facilities and Infrastructure Management
Project Management		Project Management
	Leadership in Meeting Nation's Energy Needs	

[1]According to *Major Management Challenges and Program Risks, Department of Energy* (GAO-03-100, January 2003)

[2]DOE's self-identified "Significant Issues" according to *U.S. Department of Energy Performance and Accountability Report, Fiscal Year 2002* (January 2003)

Appendix 3

RELATED REPORTS ISSUED IN FISCAL YEAR 2003

Environmental Cleanup

- Audit Report on *Treatment of Mixed Incinerable Waste* (DOE/IG-0588, March 3, 2003)
- Audit Report on *Disposal of Remote-Handled Transuranic Waste at the Waste Isolation Pilot Plant* (DOE/IG-0613, July 18, 2003)
- Audit Report on *Disposal of the Rocky Flats Environmental Technology Site's Low-Level Mixed Waste* (DOE/IG-0612, July 8, 2003)
- Audit Report on *Waste Reduction Plans for the Advanced Mixed Waste Treatment Project at the Idaho National Engineering and Environmental Laboratory* (DOE/IG-0611, July 7, 2003)
- Audit Report on *The Department of Energy's Spent Nuclear Fuel Canisters and Transportation Casks* (DOE/IG-0608, June 20, 2003)

National Security

- Audit Report on *Personnel Security Clearances and Badge Access Controls at Selected Field Locations* (DOE/IG-0582, January 24, 2003)
- Inspection Report on *Implementation of Corrective Actions Resulting From Force-on-Force Performance Tests* (DOE/IG-0585, February 12, 2003)
- Inspection Report on *The Security Afforded Selected Tritium Reservoir Shipments (U)* (DOE/IG-0619, September 16, 2003) Classified
- Inspection Report on *National Nuclear Security Administration's Ability to Meet the Aircraft Requirements of the Joint Technical Operations Team* (DOE/IG-0605, June 5, 2003)
- Audit Report on *International Materials Protection, Control and Accountability Nonproliferation Initiative* (DOE/IG-0603, June 4, 2003)
- Audit Report on *Management of the Department's Protective Forces* (DOE/IG-0602, June 3, 2003)
- Audit Report on *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 28, 2003)
- Inspection Report on *Actions Taken in Response to Missing Hazardous Waste Containing Cyanide* (DOE/IG-0592 March 21, 2003) Official Use Only

- Audit Report on *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 23, 2002)

Stockpile Stewardship

- Audit Report on *National Nuclear Security Administration's Nuclear Explosive Safety Study Program* (DOE/IG-0581, January 2, 2003)

- Audit Report on *Management of Beryllium Metal Supply* (DOE/IG-0583, January 27, 2003)

- Audit Report on *Beryllium Oxide Operations at the Y-12 National Security Complex* (DOE/IG-0595, April 16, 2003)

- Audit Report on *Savannah River Site's Waste Solidification Building* (DOE/IG-0618, September 4, 2003)

- Audit Report on *Reconfiguration of the Kansas City Plant* (DOE/IG-0616, August 13, 2003)

- Audit Report on *National Nuclear Security Administration's Planning, Programming Budget, and Evaluation Process* (DOE/IG-0614, August 5, 2003)

Contract Administration

- Special Inquiry on *Operations at Los Alamos National Laboratory* (DOE/IG-0584, January 28, 2003)

- Audit Report on *University of California's Costs Claimed and Related Internal Controls for Operation of Los Alamos National Laboratory* (DOE/IG-0596, April 16, 2003)

- Audit Report on *Transfer of Excess Personal Property from the Nevada Test Site to the Community Reuse Organization* (DOE/IG-0589, March 11, 2003)

- Audit Report on the *Oversight Funds Provided to Local Governments in the State of Nevada* (DOE/IG-0600, May 23, 2003)

- Audit Report on *Idaho National Engineering and Environmental Laboratory's Strategic Initiative Fund* (DOE/IG-0601, May 27, 2003)

- Inspection Report on *Inspection of Savannah River Operations Office Management of Emergency Response and Law Enforcement-Related Grants* (DOE/IG-0604, June 2, 2003)

- Audit Report on *Utility System Leases at the East Tennessee Technology Park* (DOE/IG-0609, June 25, 2003)

Appendix 3 (continued)

Project Management

- Audit Report on *Idaho Settlement Agreement Activities* (DOE/IG-0571, October 9, 2002)
- Audit Report on *Remote Treatment Facility* (DOE/IG-0573, November 5, 2002)
- Audit Report on *Planned Characterization Capability At The Waste Isolation Pilot Plant* (DOE/IG-0577, December 18, 2002)
- Audit Report on *Refurbishment of the W80 -- Weapon Type* (DOE/IG-0590, March 13, 2003)
- Audit Report on the *Status of the National Ignition Facility Project* (DOE/IG-0598, April 28, 2003)
- Audit Report on the *Dual Axis Radiographic Hydrodynamic Test Facility* (DOE/IG-0599 May 22, 2003)
- Audit Report on *Plutonium-238 Production* (DOE/IG-0607, June 19, 2003)

Information Technology

- Audit Report on *Business Management Information System* (DOE/IG-0572, November 4, 2002)
- Audit Report on *Information System Development Practices at the Bonneville and Western Area Power Administrations* (DOE/IG-0586, February 21, 2003)
- Interim Inspection Report on *Inspection of Internal Controls Over Personal Computers at Los Alamos National Laboratory* (DOE/IG-0597, April 24, 2003)
- Audit Report on *Security Over Wireless Networking Technologies* (DOE/IG-0617, August 25, 2003)
- Evaluation Report on *The Department's Unclassified Cyber Security Program 2003* (DOE/IG-0620, September 16, 2003)

Worker and Community Safety

- Inspection Report on *Inspection of Explosives Safety at Selected Department of Energy Sites* (DOE/IG-0578, December 19, 2002)
- Inspection Report on *Oversight of Shock Sensitive Chemicals at the Department's Ames Laboratory* (DOE/IG-0615, August 11, 2003)

IG Report No.: DOE/IG-0626

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

11

U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

The Department's Basic Protective Force Training Program

DOE/IG-0641

March 2004

Department of Energy
Washington, DC 20585

March 12, 2004

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department's Basic Protective Force Training Program"

BACKGROUND

The emphasis on homeland security and protection of national assets, especially since September 11, 2001, has prompted the Department of Energy to take a number of actions to enhance its security posture. A critical component of this effort is the cadre of over 4,000 armed personnel responsible for securing the Department's nuclear materials, weapons, and national security-related information.

The importance of the security mission, combined with a rapidly increasing number of officers, imposes a considerable burden on the Department to ensure that its protective force is well trained. For a number of years, the Department's goal has been to deliver a standardized, core curriculum designed to train its protective forces to deal with a broad spectrum of threats and to ensure interoperability across the complex.

Originally, the Department centralized the conduct of basic security police officer training at the Nonproliferation and National Security Institute in Albuquerque, New Mexico. However, in May 2001, the Department authorized individual sites to conduct basic security police officer training at their own sites, provided it was in accordance with the core curriculum. In that context, we initiated this audit to determine whether sites were meeting the Department's standardized, basic protective force core training curriculum.

RESULTS OF AUDIT

The audit disclosed that the core basic training curriculum, despite its design and purpose, had been applied inconsistently throughout the complex. At 10 of the 12 sites included in our review, significant modifications to the Department's core curriculum had been made. For example:

- Each of the 10 sites eliminated or substantially modified 2 or more blocks of instruction. At one site, about 40 percent of the required 320 hours of basic security police officer training had been eliminated by deleting courses and modifying delivery methods;

Printed with soy ink on recycled paper

- None of the 10 sites included instruction in rappelling even though it was part of the special response team core curriculum and continued to be offered by the Nonproliferation and National Security Institute;

- Only one site conducted basic training on use of a shotgun, despite the fact that a number of sites used the weapon for breaching exercises and other purposes; and,

- Seven of the sites modified prescribed training techniques by reducing the intensity or delivery method for skills that some security experts characterized as critical, such as handcuffing, hand-to-hand combat, and vehicle assaults.

We found that the Department's facilities were not required to report departures from the core curriculum to either the responsible program office or to the Office of Security. Thus, from a central perspective, there was no effective way to evaluate the impact of these actions on the national security interests of the Department. Site security managers indicated that modifications to the core curriculum had been made for reasons related to applicability or safety. However, the Department had conducted significant analyses prior to the adoption of the core curriculum as policy, including safety risk analyses.

While some level of deviation from the core curriculum to meet local conditions was understandable, the relatively large number of curriculum modifications identified during the audit raised concern as to the curriculum's validity and its usefulness as a benchmark for evaluating the performance of protective force training. In this vein, we made a series of recommendations intended to help the Department evaluate the impact of observed training modifications and determine whether the security police officer core curriculum needs to be updated. We also recommended that the Department's program offices provide additional guidance clearly defining the modifications that would require prior Departmental approval and/or notification.

Security force training has been the focus of a number of other recent Office of Inspector General reviews. In a report on *Management of the Department's Protective Forces* (DOE/IG-0602, June 2003), we noted that declining training opportunities may have affected security officer morale and retention. Also, in our inspection of *Protective Force Performance Test Improprieties* (DOE/IG-0636, January 2004), we reviewed "force-on-force" exercises at the Department's Y-12 site and determined that the training test results had been compromised.

MANAGEMENT REACTION

Consolidated comments were provided covering the views of the affected program and administrative offices and the National Nuclear Security Administration. Although the comments varied from office to office, management generally concurred with our

recommendations. Management's comments are discussed in more detail on page 6 of the report and are included in their entirety as Appendix 4.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Director, Office of Security
Director, Office of Independent Oversight and Performance Assurance

THE DEPARTMENT'S BASIC PROTECTIVE FORCE TRAINING PROGRAM

TABLE OF CONTENTS

Basic Protective Force Training Practices

Details of Finding 1

Recommendations 5

Comments 6

Appendices

1. Objective, Scope, and Methodology 9

2. Prior Reports 11

3. Core Curriculum Modifications 13

4. Management Comments 14

BASIC PROTECTIVE FORCE TRAINING PRACTICES

Background

The Department of Energy (Department), through its Nonproliferation and National Security Institute (NNSI) in Albuquerque, New Mexico, developed a standardized training curriculum for on-site training of basic security police officers and special response teams. The basic core curriculum includes critical elements that are based on the results of job analyses of major tasks and skill requirements and requires 320 hours of training. Courses, in topics such as the use of batons, handcuffs, shotguns, and hand-to-hand combat, are part of the curriculum. These training requirements were supported by risk and safety analyses and were officially adopted by the Department.

In November 1999, the Department established policy to centralize the conduct of the Basic Security Police Officer Training (BSPOT) at the NNSI. Training was centralized because of concerns over variations in delivery and to ensure uniform force readiness and interoperability among the protective forces. Subsequently, in May 2001, the Secretary authorized sites to provide BSPOT training locally to new hires, provided that training was in accordance with the current standardized Security Police Officer BSPOT curriculum. Furthermore, the Secretary specified that changes to the standardized curriculum could only be made for site-specific requirements where a portion of the curriculum was not applicable to the site. To aid in ensuring delivery of the standardized curriculum, the Office of Independent Oversight and Performance Assurance agreed to incorporate the curriculum in its site-level review.

Training and Delivery Methods

Our review disclosed that the BSPOT and the special response team [1] standardized core curriculum was being delivered inconsistently. Specifically, many sites included in our review had eliminated or modified significant portions of the training while others were not using realistic training delivery methods (see Appendix 3). At some locations, these modifications had a significant impact on the level and intensity of training. For instance, one site reduced its core training hours by about 40 percent, as a result of eliminating or modifying training in areas such as shotgun use and baton techniques.

In addition, we observed that training and practical application methods were inconsistently delivered even though the delivery methods had been previously evaluated, deemed safe, and incorporated in the core

[1] Basic special response team training is required for selected security police officers. The training is separate from, and in addition to, the basic core curriculum required for a security police officer position. Special response team members must be capable of effective, aggressive, and timely resolution of adversary actions using appropriate force and team techniques.

requirements. More than half of the sites reviewed used reduced force or instructor demonstrations, rather than realistic practical application training methods in certain areas. Officials at some sites told us that tactical skills were taught only in classroom settings or at a limited force level to avoid injuries. In particular, one site security official told us that practical application of defensive tactics such as hand-to-hand combat, take downs, or suspect restraint were performed in slow motion or at a reduced level of force. An official at another site stated that the site did not follow a specific standard for conducting defensive tactics training and permitted instructors to reduce speed or force based on needs and experience of the student. At another location, security officials indicated that the site provided no practical application in handcuffing and instead had instructors demonstrate techniques only on other instructors. Some sites also did not provide a realistic setting for vehicle assault training because they used wooden mockups or removed all vehicle glass prior to the exercise. Office of Security officials commented that sites that use unrealistic training methods did not meet Departmental requirements because the skills acquired by the officers cannot be adequately measured.

Additionally, we noted that none of the sites reviewed conducted special response team training for rappelling even though it is contained in the required curriculum for special response team members and is currently taught by the NNSI. Security officials disagreed on the importance of this training module. Following a fatal accident in 1995, sites eliminated rappelling from special response team training because of concerns over safety and the importance of the skill to mission needs. A security official told us that a Quality Panel had recommended eliminating rappelling from the core curriculum because sites no longer included it in their special response team training, however, rappelling remains part of the core curriculum. Office of Security officials told us that rappelling training was important for team and confidence building skills and that it had been the subject of a safety risk analysis. As a result, NNSI continues to provide the training and has trained approximately 434 officers in rappelling since 1998. We were not provided a full and definitive explanation for the inconsistent application of the training requirement for rappelling.

Core Curriculum

Modifications to the core curriculum and the training delivery methods occurred because site security managers eliminated certain courses in response to applicability or safety concerns. However, these variations were not always detected or their impact on readiness assessed because the Department did not require the sites to report departures from the core training requirements to either the responsible program office or the Office of Security.

Site-Level Modifications

Sites excluded or modified certain courses from the standardized core curriculum in response to applicability or safety concerns. This despite the fact that NNSI conducted safety risk analyses for each of the courses in the standardized core curriculum. For example, a number of sites excluded shotgun and baton training because those items of equipment were not used at their site. Additionally, sites routinely utilized alternative methods in performing certain tactical exercises due to safety considerations. As previously discussed, certain sites deviated from the curriculum by eliminating glass windshields during vehicle assault training because of concerns related to shattering glass. However, we were told that the glass windshields provided a realistic setting so that protective force trainees could obtain a better understanding of ballistic and refraction properties.

Certain sites determined that courses were unsafe while others delivered the same courses without modification. SO training officials indicated that they were aware of the inconsistencies and informed us that they could not understand how personnel at one site could deem a practice acceptable while others would refuse to administer the block of training using prescribed levels of force. In some of these cases, Department and contractor security officials indicated that site management was concerned because there was a correlation between the number of injuries incurred at a site and the contractor's performance evaluation rating and subsequent fee determination. At some sites instructors were specifically told to limit force used during training to avoid injuries.

Approval and Reporting Guidance

We further noted that Federal managers could not assess the impact of training changes on the Department's goal of uniform force readiness because sites were not required to report to program offices or the Office of Security on modifications made to the core curriculum. A few of the sites we reviewed had requested and received approval from the Office of Security to modify the standardized core curriculum. However, officials at other sites told us that they were not required to go through an approval process before eliminating courses not considered applicable to their site or for safety reasons. Additionally, some site-level security officials indicated that as long as the course goal was satisfied, they were free to modify delivery methods as they saw fit.

The Office of Security, which has policy responsibility for security police officer training, indicated that modifications did not require approval other than at the site-level. Based on information they gathered, Office of Security officials believed that site-level security managers should be fully cognizant of departures from the core curriculum because such changes were approved by Federal officials as part of the site's annual training program. Our review of these training programs, however, disclosed that they frequently lacked detail necessary to identify or inform management or program officials of significant changes in the level of training intensity. In fact, a National Nuclear Security Administration (NNSA) official indicated that they were unable to fully assess the impact on the training programs and force readiness because they were not provided with specific information regarding modifications to site-level training programs. Additionally, Office of Science program officials pointed out that the modifications in training curricula and differences in training delivery methods should be identified and monitored by the programs.

Core Curriculum Integrity

We also determined that the Department had not specifically reviewed site-level training programs to ensure that they conformed to the core curriculum. Based on a Department analysis completed in 2001, the Secretary authorized sites to conduct new-hire basic security police officer training provided they adhered to the core curriculum. As previously discussed, the Department's Office of Independent Oversight and Performance Assurance (OA) agreed to incorporate the basic training curriculum as a topical area in its reviews of site-level programs. Even though OA includes certain aspects of the BSPOT in their assessments of the site protective force training programs, to date, they have been unable to begin curriculum reviews because of a workload increase associated with the events of September 11, 2001. Such reviews could identify core curriculum modifications and assist the Department in assessing safety and applicability concerns expressed by site security officials.

Force Readiness

Inconsistent training methods may increase the risk that the Department's protective forces will not be able to safely respond to security incidents or will use excessive levels of force. As noted by NNSI and a private protective force organization, most tactical skills can only be learned by repetitive practice in an appropriately realistic setting. Specifically, defensive tactics training should be as realistic as possible. Anything less may rob the trainee of the exposure to the

levels of force, panic, and confusion that are usually present during an actual attack and increase the possibility of an inappropriate response in high stress situations.

RECOMMENDATIONS

We recommend that the Under Secretary for Energy, Science and Environment, and the Administrator, National Nuclear Security Administration:

1. Determine the extent of and reasons for curriculum modifications and differences in training delivery methods throughout the Department's complex; and,

2. Provide additional guidance, based on the above determination, defining modifications requiring prior Departmental approval and/or notification.

We recommend that the Director, Office of Security:

3. In conjunction with the program offices and the information gathered in response to Recommendation 1, complete evaluations of the applicability of the current core curriculum for basic security police officers and special response team training to ensure that training is properly aligned with job and policy requirements; and,

4. Request that the Assistant Secretary for Environment, Safety and Health review the safety oversight of protective force training activities to ensure there is consistency in safety oversight as it relates to protective force training.

We recommend that the Director, Office of Independent Oversight and Performance Assurance:

5. Incorporate basic security police officer training as a topical area of review in all future field activity reviews as discussed in the Secretary's memorandum of May 2001 .

MANAGEMENT REACTION

The Offices of Security; Science; Environmental Management; Nuclear Energy, Science and Technology; Independent Oversight and Performance Assurance; and Environment, Safety and Health, along with the NNSA commented on a draft of this report. Comments from the responding organizations varied in degrees of concurrence and non-concurrence on the draft report's recommendations. Overall, the program offices concurred with the recommendations to review curriculum modifications and differences and to issue additional guidance defining Departmental notification levels. NNSA also strongly supported a review of the protective force core curriculum to ensure that it met current requirements that include changes in mission and threat scenarios.

The Office of Security fully concurred with the recommendation to include basic security training as a topical area of review by OA. However, it stated that the recommendation on evaluating the applicability of the core curriculum was not needed because "such an evaluation is conducted on a practically on-going basis and the curricula is current." The applicable protective force job analyses and curricula have been reviewed and updated by the NNSI and the Office of Security quality panels. As an example, the Office of Security pointed out that the NNSI is conducting a comprehensive review of the BSPOT curriculum to ensure it meets current job task analyses and mission requirements.

Finally, the program offices and the Office of Security pointed out the need for the sites to be able to modify their training programs to reflect their job and mission needs. The Office of Security also indicated that security police officers supporting mission requirements at other sites is not an issue for training because (1) labor issues prohibit security police officers who are members of bargaining units from acting as augmentees at other sites, and (2) augmentees would receive site-specific training before commencing work at another site. Management's consolidated comments to this report have been incorporated verbatim in Appendix 4. Based on management's comments, where appropriate, adjustments have been made to the body of the report and the recommendations.

AUDITOR COMMENTS

Management comments were generally responsive to our recommendations.

Regarding the Office of Security's disagreement with the need for the recommendation on evaluating the applicability of the core curriculum,

we believe that the NNSI and Office of Security evaluations cited above should continue. Furthermore, the evaluations should be conducted in conjunction with the program offices and reflect information gathered by those offices regarding how sites have modified the core curriculum and the reasons for the modifications. The intent of the recommendation is to evaluate the standardized core curriculum developed by the NNSI, and approved by the Department; to determine which portions of the training, if any, should be eliminated; and to determine if training is properly aligned with Departmental job and policy requirements.

Based on the number of modifications that we identified during the audit, we believe that changes may need to be made to the core curriculum, or sites may need to revisit their modifications of the curriculum. We recognize that quality panels play an important role in evaluating the core curriculum; however, they can only recommend that changes be made. The Office of Security has the final approval over any recommended changes. As previously discussed, in the case of rappelling, there is a difference of opinion among security officials about the importance of this training block. In spite of this disagreement, NNSI continues to include rappelling training in the core curriculum, but no other site is instructing that portion of the curriculum.

We have modified the recommendation pertaining to safety oversight to reflect the Office of Security's concerns about the consistency of protective force training safety oversight. However, it is, in our judgment, the Office of Security's responsibility to request a review by the Assistant Secretary for Environment, Safety and Health because the initial safety risk analyses supporting the core curriculum were conducted by the NNSI.

Regarding concerns expressed by the program offices and the Office of Security that sites have the authority to modify the core curriculum to meet their specific needs, given the Department's ongoing commitment to enhancing security at its key facilities, such modifications should have higher level visibility as envisioned in the first two recommendations. In that regard, we recognize that the Secretary of Energy's May 15, 2001, memorandum permits sites to conduct new hire BSPOT training and allows sites to make changes to the standard curriculum for site-specific requirements where a portion of the curriculum is not applicable. However, that memorandum, as well as relevant Department orders, were issued prior to the events of

September 11, 2001. Since then, the emphasis on homeland security and the protection of national assets has increased significantly. For example, the Department has developed a new Design Basis Threat - policy and has increased the number of protective force personnel by about 500 officers. Additionally, it has been the Department's policy to train its security forces to deal with a broad spectrum of threats by providing a standardized, core training curriculum that ensures interoperability across the complex.

Regarding the Office of Security's position that interoperability of the protective forces is not a training issue, we disagree. Specifically, a work stoppage caused by labor issues is only one event that could necessitate the transfer of protective forces to another site. Other events, non-labor related, could lead to the transfer of protective forces and not provide the time to train the augmentees in the specific site's equipment or needs.

Appendix 1

OBJECTIVE

To determine whether sites were meeting the Department's standardized, basic protective force core training curriculum.

SCOPE

We conducted the audit from February 2003 to September 2003, at Department of Energy Headquarters in Washington, DC; the Nonproliferation and National Security Institute in Albuquerque, New Mexico; the Oak Ridge Complex in Oak Ridge, Tennessee; the Lawrence Livermore National Laboratory in Livermore, California; and the Nevada Test Site in Nye County, Nevada. We also interviewed officials from the following organizations:

Federal Law Enforcement Training Center, Cheltenham, MD
National Aeronautics and Space Administration
Department of State
Nuclear Regulatory Commission

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable Federal regulations, Departmental orders, and implementing procedures and practices;
- Reviewed performance evaluation reports and/or performance measures at selected sites;
- Reviewed protective force annual training budgets at selected sites;
- Obtained and reviewed Office of Security strength reports since 1992;
- Obtained and reviewed the National Nuclear Security Administration quarterly strength report for April 2003;
- Collected and analyzed training hours and cost data for the Nonproliferation and National Security Institute;
- Collected and analyzed training hours and cost data for 12 of the Department's sites:
  - Lawrence Livermore National Laboratory,
  - Nevada Test Site,
  - Oak Ridge Complex,

- Rocky Flats Environmental Technology Site,
- Hanford Site,
- Pantex Plant,
- Savannah River Site,
- Los Alamos National Laboratory,
- Idaho National Engineering and Environmental Laboratory,
- Sandia National Laboratories (New Mexico),
- Sandia National Laboratories (California), and
- Sandia National Laboratories (Tonapah Test Range);

- Reviewed performance related information to determine compliance with the Government Performance and Results Act of 1993;

- Held discussions with Headquarters and other Federal Government officials regarding the Department's protective forces; and,

- Held discussions with officials from Lawrence Livermore and Oak Ridge National Laboratories, as well as, the Nevada Test Site and the Nonproliferation and National Security Institute regarding protective forces.

The audit was performed in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Accordingly, the assessment included reviews of Departmental and regulatory policies, procedures, and performance measures related to the Department's protective forces. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not conduct a reliability assessment of computer-processed data because only a very limited amount of computer-processed data was used during the audit.

The exit conference was held with management on March 1, 2004.

Appendix 2

PRIOR AUDIT REPORTS

Office of Inspector General Related Reports

- *Management of the Department's Protective Forces* (DOE/IG-0602, June 2003). Although the Department had taken steps to improve the management of its protective forces, it still faced a number of challenges that could adversely affect the program. These challenges included delays in processing security clearances, increasing overtime costs, potential retention problems, and operational vulnerabilities associated with unscheduled work stoppages. Management generally concurred with the findings and recommendations and agreed to initiate corrective actions.

- *The Restructure of Security Services by the Oak Ridge Operations Office* (DOE/IG-0487, October 2000). The Oak Ridge Operations Office (Operations Office) did not manage the restructuring of its security services in a way that would have achieved its goals. Specifically, the Operations Office did not perform an analysis of security service staffing levels, determine the scope of work to be transferred, or develop cost-reduction measures or incentives to ensure efficient contractor performance. In addition, the Operations Office did not consider cost as a ranking factor in the selection of security services. Management concurred with the finding and recommendations and agreed to initiate corrective actions.

- *Audit of Construction of Protective Force Training Facilities at the Pantex Plant* (WR-B-95-06, May 1995). Construction of a physical training facility at the Department's Pantex Plant was not necessary to fulfill mission needs, and the Department did not consider all viable alternatives to constructing a weapons tactics and training facility. These conditions occurred because a Justification for New Start was never prepared and approved for these two projects. Management did not concur with all of the recommendations.

- *Audit of the Department of Energy's Security Police Officer Training* (CR-B-95-03, February 1995). The audit disclosed that the Department had not established standardized annual refresher training requirements for its security forces and individual sites were developing and implementing training programs and course plans without emphasis on standardization.

- *Audit of the Management and Cost of the Department of Energy's Protective Forces* (DOE/IG-0354, July 1994). The audit noted several opportunities for the Department to improve the operational efficiency of the protective forces, including eliminating overtime paid to officers prior to completion of the basic 40-hour workweek. Management concurred with the findings and recommendations and agreed to take appropriate actions to improve the efficiency of managing protective forces.

- *Management of the Central Training Academy, Albuquerque, New Mexico* (DOE/IG-0309, May 1992). The audit disclosed that Wackenhut (1) was provided credentials and shields that improperly identified employees as being Federal agents and officers, and used the Department's official seal without proper authorization, (2) incurred costs not necessary for performing contract work, (3) performed work outside the general scope of its contract, and (4) operated a souvenir store on Government property. All of these activities occurred with the knowledge of Department officials. Management generally agreed with the findings and recommendations.

General Accounting Office Related Reports

- *Nuclear Security, NNSA Needs to Better Manage Its Safeguards and Security Program* (GAO-03-471, May 2003). NNSA has not been fully effective in managing its safeguards and security program in four key areas. As a result, NNSA cannot be assured that its contractors are working to maximum advantage to protect critical facilities and material from individuals seeking to inflict damage. The four areas are as follows: (1) Defining clear roles and responsibilities; (2) Assessing sites' security activities; (3) Overseeing contractors' corrective actions; and (4) Allocating staff. NNSA disagreed with GAO's conclusion that NNSA was not ensuring the comprehensive, annual assessments of contractors' performance that DOE policy requires. GAO continues to believe that NNSA's current efforts do not ensure conformance to DOE policy.

- *Department of Energy, Key Factors Underlying Security Problems at DOE Facilities* (GAO/T-RCED-99-159, April 1999). Physical security controls involve the protection, primarily through security personnel and fences, of facilities and property. In 1991, GAO reported that security personnel were unable to demonstrate basic skills such as the apprehension and arrest of individuals who could represent a security threat. Prior to that report, in 1990, GAO reported that weaknesses were occurring with security personnel, as some security personnel could not appropriately handcuff, search, or arrest intruders or shoot accurately.

Appendix 3

Core Curriculum Modifications by Site

X indicates a modification has been made to curriculum

Site Locations	Shotgun	Baton	Rappelling	Modified Defensive Tactics	Other courses excluded or modified
Lawrence Livermore National Laboratory	X		X	Information not available at time of audit	
Nevada Test Site	X	X	X		Vehicle assaults
Oak Ridge Complex	X	X	X		
Rocky Flats Environmental Technology Site	X		X	X	
Hanford Site		X	X	X	Moving vehicle assault
Sandia National Laboratories (California)	X		X		Rifle, vehicle stops, aerosol/chemical spray
Pantex Plant	X	X	X	X	
Savannah River Site	X		X	X	Vehicle assaults
Los Alamos National Laboratory	X	X	X	X	Reloading drills
Idaho National Engineering and Environmental Laboratory	X		X	X	Vehicle assaults

NOTE: Training at Sandia National Laboratories (New Mexico and Tonopah Test Range) was not conducted on-site, therefore was not included in the above chart.

Department of Energy
Washington, DC 20585

NOV 07 2003

MEMORANDUM FOR FREDERICK D. DOGGETT
ASSISTANT INSPECTOR GENERAL
FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM: Marshall O. Combs
MARSHALL O. COMBS, ACTING DIRECTOR
OFFICE OF SECURITY

SUBJECT: Consolidated Comments on Office of Inspector General Draft Audit Report, *The Department's Basic Protective Force Training Program*

Below, for your review are the Department's consolidated comments to the above subject draft report. These comments are very brief and general in nature as a result of your direction to attempt to limit the Department's "Management Reaction" to only two pages. However, as permitted, you will also find attached each responding organization's detailed and unabridged comments for your review and consideration. As you will see, there are varying degrees of concurrence and non-concurrence on the draft report's recommendations from the responding organizations.

The Office of Security (SO) Comments.

Regarding sites deviating from protective force (PF) "core curricula," the Department of Energy (DOE) directives require that all PF training be based on site-specific job analyses (JAs) of PFs' assigned duties and criteria established by the DOE Nonproliferation and National Security Institute (NNSI)/Central Training Academy (CTA). In May 2001, the Secretary of Energy authorized sites to conduct basic PF training, while meeting specific criteria and allowed changes to be made to the standard curriculum for site-specific requirements where a portion of the curriculum is not applicable. In response to a Type A, Accident Investigation Board, investigating a PF rappelling fatality, all rappelling operations at DOE sites were suspended in 1995. Based upon lessons learned from the investigation, the sites were required to review their rappelling operations to ensure they were mission-essential. As a result, all sites determined rappelling was not required to meet site response mission requirements. Therefore, if the sites' PF JAs do not identify a portion of a curriculum as a site-specific PF task or mission requirement, then the sites are not required to teach it.

Deviations are required, by policy, to be submitted where it is justifiable to not meet a directive's requirement. While basic PF training is based on criteria

Printed with soy ink on recycled paper

established by the NNSI CTA (the approved curricula), this criteria is not a directives requirement. There is no existing DOE requirement for sites to submit a "deviation" request in order to depart from the standard PF curriculum. Finally, DOE directives require that site PF training programs be approved by the cognizant local DOE authority for safeguards and security, which also has the direct responsibility to ensure the training is properly implemented as required.

It is SO's position that Draft Recommendation 3 is not applicable and should be revised to read: ". . . the Under Secretary for Energy, Science and Environment, and the Administrator, National Nuclear Security Administration (NNSA): . . . Ensure that the cognizant local NNSA and Program Office officials that are responsible for oversight of PFs conduct a thorough review of their respective PFs annual training plans to ensure that all applicable core curriculum and site-specific areas are included, prior to the annual training plan's approval."

It is SO's position that Draft Recommendation 4 is not applicable and should be deleted due to the fact that the applicable PF JAs and curricula have been reviewed and updated regularly by the NNSI and SO PF Quality Panels.

It is SO's position that Draft Recommendation 5 should be revised to state: "We recommend that the Assistant Secretary for Environment, Safety, and Health: . . . Conduct a review of the safety oversight of sites' PF training activities to ensure there is standardization, that oversight is implemented in a consistent manner at all sites conducting the same types of operational and training activities, and the use of PF injury/illness rates in PF contract award fee determinations is being appropriately applied."

The Office of the Assistant Secretary for Environmental Management.

Recommendation 1. The report identifies sites as deviating from the core curriculum for basic PF officer and special response teams. It is this Office's understanding that as a result of the rappelling death in 1995, the Department issued a notice to cease all rappelling activities. The sites should not be penalized for following the Department's guidelines. Another issue identified in the report is that shotgun training is not being conducted at all sites. During the developmental stages of the PF training program, it was decided that each course of instruction would be conducted only if applicable to the site.

Recommendation 2. As a result of this report, it is clear that the Department needs to define the process for deviating from the basic curriculum. It is the Department's responsibility to provide clear guidance as to whether the approved deviation process is to be followed, or, if not, what process is to be used.

Recommendation 3. The Department's approved deviation procedure identifies the proper reporting channels. If the deviation process (or a similar process), is to

be used for deviating from the PF training curriculum, it should be followed and enforced.

The Office of Nuclear Energy, Science and Technology Comments.

"The report should specify the sites included in the review. The results section indicates that 12 sites were reviewed; however, in the scope description only the Oak Ridge Complex, Lawrence Livermore National Laboratory, and the Nevada Test Site are noted."

The Office of Science (SC) Comments.

The draft report does not address the PF job task analyses and training needs assessments that help define each site's Training Approval Program (TAP). These analyses form the basis for the mode, frequency, and duration of blocks of instruction, and provide opportunities for sites to tailor training programs to site-specific conditions.

In the Secretary of Energy's memorandum dated May 15, 2001, deviations from the standardized basic PF curriculum were authorized when aspects of the training were determined to be not locally applicable. The TAP process validates these determinations. In the case of the SC PF training program at the Oak Ridge complex, deviations from the standardized curricula were approved by SO in August 2001.

The first two recommendations appear reasonable; however, SC sees no need for the development of additional procedures (Draft Recommendation 3) to further explain that which is clearly delineated in DOE Order 470.1 -- and which would be reiterated in the guidance promulgated by Recommendation 2 -- regarding requirements for processing and approving deviations.

The Office of the Associate Administrator for Management and Administration, National Nuclear Security Administration Comments.

A manifestation of increased efforts in protective measures and their associated costs relative to overtime wages has been the trade-off in training hours for overtime hours. The NNSA will use the recommendations within this report to increase the focus on training, and to resume appropriate levels and types of training.

Overall, the NNSA agrees with the recommendations in the report. As part of NNSA's reengineering effort, it is defining roles and responsibilities, and issuing clarifications, via NNSA policy letters, to existing Departmental directives. The process for submitting deviations will be reiterated to all NNSA field elements.

Augmentee forces are trained in site-specific weapons and tactics upon arrival and prior to performing their duties. Arrangements are made in advance to do this. Experience has taught that these perishable skills are more beneficial when learned on a "Just In Time" basis using site-specific equipment.

A review of the PF core curriculum is strongly supported. Currently, many sites are using curricula tailored to site-specific needs. Changes in mission and threat scenarios warrant a thorough review of the curriculum to meet today's requirements.

The Office of Environment, Safety, and Health Comments.

This Office informed SO that it did not have any comments to the subject draft report.

Should you have any questions regarding this subject, please contact Mr. Ronnie Edge, of my staff, at (301) 903-4247.

Attachments

Department of Energy
Washington, DC 20585

November 4, 2003

MEMORANDUM FOR: Gregory H. Friedman
Inspector General
Office of Inspector General

FROM: Glenn S. Podonsky, OA-1

SUBJECT: Inspector General Report on Basic Security Police Officer Training Program

We appreciate the opportunity to review and comment on your report summarizing the results of the Basic Security Police Officer Training (BSPOT) Program audit. We generally agree with the findings and recommendations in the report. However, as stated in our previous comments on the draft report, OA does review some elements of the BSPOT program as part of the overall review of site training programs for protective forces. Specifically, OA evaluates the site's Training Approval Program (TAP), which includes elements of the BSPOT program, such as annual training plans, course objectives, instructor qualifications and weapons training. Our current approach should be added to the report for factual accuracy.

We note that the recommendation made to OA in the audit report suggests expanding our review of the BSPOT program. We also recognize the value of this approach. Our proposed steps are to continue reviewing the site BSPOT programs by evaluating site vulnerability assessments, safeguards and security plan development, and response/protection strategy in determining the appropriateness of established training needs, individual protective force member job task analyses and assessing the quality of the actual training being conducted. In addition, we plan to analyze the Nonproliferation and National Security Institute (NNSI) core BSPOT curriculum and compare the core program with the site BSPOT curriculum, where applicable. Not all sites have a BSPOT program since some sites rely on NNSI for this training. Where site training programs deviate from the core curriculum, we will assess if the differences make sense based on the sites' protection missions.

We appreciate your suggestions. I am available to discuss this matter further at your convenience.

Glenn S. Podonsky, Director
Office of Independent Oversight
and Performance Assurance

cc:
R. Speidel, NN-66
M. Kilpatrick, OA-1

Printed with soy ink on recycled paper

IG Report No.: DOE/IG-0641

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

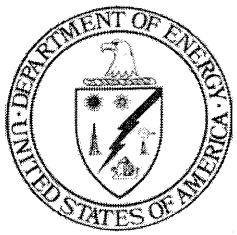
If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

12



U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Special Report

Management Challenges at the Department of Energy

DOE/IG-0667

November 2004

Department of Energy

Washington, DC 20585

November 30, 2004

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Report on "Management Challenges at the Department of Energy"

BACKGROUND

In 1997, the Office of Inspector General began an annual effort to identify what it considers to be the most significant management and performance challenges facing the Department of Energy. Now codified as part of the *Reports Consolidation Act of 2000,* this effort highlights those programs and operations that are, in our judgment, inherently the most difficult to manage and those with demonstrated performance problems. We reach these judgments based on an assessment of the agency's progress in addressing previously identified challenges and relevant work performed by the Office of Inspector General. We also consider emerging issues facing the Department. The process is continually refined, and in 2004 we began to categorize management challenges as either mission-related or internal control oriented. We also developed a watch list that reflects operational or programmatic functions that, in our view, need to be closely monitored by Department management.

RESULTS

In our previous report, *Management Challenges at the Department of Energy* (DOE/IG-0626, November 2003), we identified six management challenges. The Department has taken significant positive steps to address these challenges; however, we concluded that these challenges continue as the most serious risks facing the Department in 2005 and beyond. Each of these challenges has been a long-standing and widely acknowledged issue for the Department of Energy.

Mission-Related Challenges

- National Security
- Environmental Cleanup
- Stockpile Stewardship

Internal Control Challenges

- Contract Administration
- Project Management
- Information Technology

Printed with soy ink on recycled paper

For the most part, the challenges are not amenable to simple, near-term resolution and can only be addressed by a concerted, persistent effort, resulting in progress over a long period of time. As we reported last year, three challenges are associated with mission-related activities and three challenges are associated with weaknesses in the Department's internal control structure. Specifically, mission-related challenges represent risks that are inherent to the Department's complex operations and are likely to persist well into the future, in part, because they involve factors that are largely outside of the Department's direct control. Internal control challenges relate to weaknesses in the Department's management processes which, if not addressed, may impede the Department's ability to carry out its program responsibilities and to ensure the integrity of its operations.

We noted that under your leadership the Department has continued its initiative, started in March 2003, to address the identified management challenges. The Deputy Secretary, as the focal point of this initiative, has been personally invested in its operation, working with the Under Secretaries and Assistant Secretaries to achieve progress. Based on our analysis of this effort, if this initiative continues with the personal involvement of the Department's senior leadership, the risks associated with the identified management challenges should be reduced.

Further, the Department is actively addressing the President's Management Agenda to make the Federal government more efficient, effective, results-oriented, and accountable to the citizens who pay taxes and benefit from the programs and services government provides. As you reported in *Energizing America for a New Century*, the Department has made the President's Management Agenda its own. The Office of Management and Budget has ranked the Department as one of the top cabinet-level agencies in demonstrating progress in the implementation of the President's Management Agenda. The Department's progress and success to date in adopting the Agenda's principles should contribute significantly to mitigating the Department's challenges in the long term.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science and Environment
Administrator, National Nuclear Security Administration
Director, Office of Management, Budget and Evaluation/Chief Financial Officer
Chief of Staff

SPECIAL REPORT ON MANAGEMENT CHALLENGES AT THE DEPARTMENT OF ENERGY

TABLE OF CONTENTS

Analysis of Management Challenges

Background 1

Mission-Related Challenges 1

Internal Control Challenges 8

Appendix

1. Watch List 15

2. Table Comparing Management Challenges Reported by Various Groups 18

3. Related Reports Issued in Fiscal Year 2004 19

Background

The Department of Energy (Department) missions encompass a broad range of areas vital to our national security and economic well-being including nuclear security, environmental quality, science, and energy resources. To accomplish its missions, the Department receives annual appropriations of about $23 billion, employs about 14,000 Federal and 100,000 contractor personnel and manages more than $115 billion of assets.

As required by the *Reports Consolidation Act of 2000*, this report documents the Office of Inspector General's judgment as to the most serious management challenges facing the Department. Beginning last year, we categorized challenges as either mission-related or internal control.

Although the Department has taken significant positive steps to address the six management challenges identified last year, we continue to consider these challenges to be the most serious risks facing the Department. Our conclusions are drawn primarily from our audits, inspections and investigations of the Department and its operations, but also consider other sources of data.

Mission-Related Challenges

We continue to identify National Security, Environmental Cleanup, and Stockpile Stewardship as long-standing mission-related management challenges. These challenges represent the risks inherent in the complex, and often cutting edge, operations that the Department must undertake to accomplish its missions. Indeed, these challenges will persist into the future because they are not amenable to short-term solutions, and they often involve factors that are outside of the Department's direct control.

National Security

As in previous years, we have identified national security as a significant management challenge due to both the criticality of the Department's operations and the continuing nature of security threats. The Department must ensure that its most sensitive materials, facilities, and information are secure and protected from hostile groups or countries.

During Fiscal Year (FY) 2004, the Department continued to address security issues. For example, Design Basis Threat implementation plans were approved for each National Nuclear Security Administration (NNSA) site. These plans identify the actions considered necessary to upgrade site security posture in

order to meet the Secretary's mandate to be in compliance with the new Department-wide Design Basis Threat Policy by the end of FY 2006. In May 2004, to further strengthen security enhancements that were instituted after the September 11, 2001, attacks, the Secretary announced major security initiatives to bolster protection for the Department's sensitive information and facilities containing special nuclear material. Moreover, in June 2004, the Department issued Order DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, to enhance the requirements, approval process, and tracking mechanism for visits and assignments by foreign nationals to Department sites or involving Department information or technologies.

In an effort to reduce the threat of nuclear weapons proliferation, the Department had initiated the Foreign Research Reactor Spent Nuclear Fuel Acceptance Program to recover foreign research reactor spent fuel containing highly enriched uranium produced in the U.S. In our audit of the program, *Recovery of Highly Enriched Uranium Provided to Foreign Countries* (DOE/IG-0638, February 2004), we concluded that as of August 2003, the Department was likely to recover only about half of the approximately 5,200 kilograms of highly enriched uranium covered by the Program and there was no effort to recover an additional 12,300 kilograms dispersed to foreign countries which were not included in the Program. The Department has taken positive steps in response to our audit by forming a multi-program working group within the Under Secretary's office to address enriched uranium and placing a priority on accepting eligible material from reactors and countries where the material may pose environmental or proliferation risks.

Although progress has been made, recent incidents and our audits and inspections have underscored the need for continued vigilance and emphasis on security issues. For example, a July 2004 inventory at Los Alamos National Laboratory revealed that two zip discs containing classified material could not be located. The Secretary responded swiftly to this incident and ordered all Department facilities to stand down operations concerning classified removable electronic media (CREM) until complete and accountable custodial responsibility for CREM was established with complete inventories, appropriate training, and security procedure reviews.

We have also identified weaknesses in the Department's and its laboratories' ability to assure that laptop, desktop, and related equipment are appropriately controlled and adequately safeguarded

from loss or theft and that classified computer use met security standards. For example, our inspection of *Internal Controls Over the Accountability of Computers at Sandia National Laboratory, New Mexico* (DOE/IG-0660, August 2004) observed that Sandia used computer peripherals for classified processing without appropriate accreditation and had not effectively implemented property management controls for computers built in-house. Our inspection report on *Internal Controls Over Classified Computers and Classified Removable Media at the Lawrence Livermore National Laboratory* (DOE/IG-0628, December 2003) disclosed that classified Nuclear Emergency Search Team computer equipment and removable media were not subjected to required inventories, six classified desktop computers remained in property inventory even though they were no longer at the site, and a classified removable hard drive was not entered into the tracking and accounting system.

Further, the Department and its contractors rely upon protective force personnel to secure and protect facilities that produce, store, and handle significant quantities of nuclear materials, weapons, and national security-related information. Our reviews concerning the readiness of the Department's protective forces identified needed improvements at sites that represent some of the most critical national security components in the Department's complex. In our inspection report on *Protective Force Performance Test Improprieties* (DOE/IG-0636, January 2004), we confirmed concerns of a Site Manager that the results of a protective force performance test conducted in June 2003 may have been compromised and, in our opinion, should not be relied upon. Our audit of *The Department's Basic Protective Force Training Program*, (DOE/IG-0641, March 2004) found that the Department's standardized, basic protective force core training curriculum had been applied inconsistently throughout the complex. While some level of deviation from the core curriculum to meet local conditions was understandable, the relatively large number of curriculum modifications identified during the audit raised concern as to the curriculum's validity and its usefulness as a benchmark for evaluating the performance of protective force training. In our inspection report on *Reporting of Security Incidents at the Lawrence Livermore National Laboratory* (DOE/IG-0625, November 2003), we concluded that Livermore did not ensure that security incidents involving missing master keys and master Tesa cards were reported within required timeframes, nor were timely follow-up actions taken to identify and address potential security vulnerabilities resulting from the incidents.

In our audit of *The Department's Continuity Planning and Emergency Preparedness* (DOE/IG 0657, August 2004), we reported that the five sites reviewed had not developed comprehensive plans to continue essential functions during an emergency and had not corrected a number of weaknesses identified during emergency preparedness exercises. Additionally, the Department had not required sites to validate the effectiveness of corrective actions for addressing recognized emergency preparedness weaknesses or to share lessons learned about common problems. As a result, the Department may face increased risks to its operations, employees, and surrounding communities during an emergency situation. In our audit of *Safeguards Over Sensitive Technology* (DOE/IG-0635, January 2004), we found that, at the three national laboratories included in our review, available controls over sensitive technologies had not been employed in all instances.

Environmental Cleanup

Environmental cleanup, including nuclear waste disposal, is a long-term management challenge faced by the Department. The Department is charged with the complex and costly task of protecting human health and the environment by cleaning up sites that supported nuclear weapons research, testing, and production activities. It must also address the need to permanently dispose of defense-related high-level radioactive wastes as well as spent nuclear fuel from civilian nuclear power plants.

The Department has made significant strides in developing and implementing a strategy to reduce the risks associated with environmental cleanup and nuclear waste disposal. For example, in June 2004, the Office of Environmental Management (EM) issued the *Office of Environmental Management Closure Planning Guidance* which, based on EM's Top-to-Bottom-Review, formalized processes intended to deliver results and safely complete cleanup of the EM program by 2035. This document established measurable cleanup objectives, goals, and performance expectations for each organizational element within EM. In addition, in FY 2004, the Department established the Office of Legacy Management which has the responsibility to ensure protection of human health and the environment through long-term stewardship of land, structures, facilities, and records. This Office will also oversee the Department's post-closure responsibilities for former contractor employees. However, the Department's

environmental cleanup progress could be hindered by litigation challenging the Department's Waste Incidental to Reprocessing authority.

Our work in FY 2004 pointed out issues concerning the Department's ongoing cleanup efforts. For example, in our audit of *Transuranic Waste Retrieval and Processing at the Hanford Site* (DOE/IG-0624, October 2003), we concluded that Department milestones were in jeopardy because sufficient emphasis had not been placed on projects for retrieving and processing waste. The Department had not established what we considered to be an achievable transuranic waste retrieval plan and had not performed a comprehensive study to determine obtainable retrieval rates and optimal processing levels to meet, at minimal cost, regulatory milestones and cleanup goals. Our audit of the Department's planned facilities for *Depleted Uranium Hexafluoride Conversion* (DOE/IG-0642, March 2004) found that the Department has an opportunity to save at least $55 million by adding an additional conversion line at the Portsmouth, Ohio facility. In addition, our report on *Groundwater Remediation Activities at Hanford* (DOE/IG-0655, July 2004) noted that the Department had not made significant progress in its efforts to remediate groundwater at the Hanford Site and that pump-and-treat systems installed in 1995 for that purpose have been largely ineffective. At Hanford, the Department risks further contamination of the groundwater and continued expenditure of funds on a largely ineffective technology.

In 1994, the Defense Nuclear Facilities Safety Board recommended that the Department stabilize fissionable and radioactive materials at Los Alamos National Laboratory and at numerous other Department sites in order to reduce safety and health risks to Department employees and the public. In our audit, *The Stabilization of Nuclear Materials at Los Alamos National Laboratory* (DOE/IG-0659, August 2004), we noted that although the Department has made some progress in stabilizing the most hazardous fissionable materials, stabilization has not been accelerated to the level anticipated and will not be completed until 2010, well beyond the original projected completion date of 2002. Unless the Department and Los Alamos place a higher priority on stabilizing these materials, radioactive materials at the Laboratory may continue to deteriorate, negatively impact the safety and health of workers, and increase costs to stabilize these dangerous materials.

In the area of nuclear waste disposal, we noted that the President designated Yucca Mountain as the site for the nation's first safe

repository. The Administration believes that the successful completion of the Yucca Mountain project will ensure that the United States has a safe and secure underground facility that will store nuclear waste in a manner that is protective of the environment and American citizens. The goal of accepting waste into the repository could be affected by various issues such as funding, regulatory rulings, and legal challenges.

Before the licensing process for Yucca Mountain is to begin, the Department is required to publicly disclose all relevant documents by posting them on the Department's public website which is accessible through the internet based Licensing Support Network sponsored by the Nuclear Regulatory Commission. Our audit, *Management Controls Over the Licensing Support Network for the Yucca Mountain Repository* (OAS-M-04-04, May 2004), observed that the Department had made significant progress in preparing licensing related information for public disclosure on the Network. However, we identified obstacles that the Department still faces in preparing the Network for initial certification and ensuring that documents are available for public review on a timely basis.

Stockpile Stewardship

The Department's Stockpile Stewardship Program is responsible for maintaining the safety, reliability, and performance of the nation's nuclear weapons stockpile in the absence of underground nuclear testing. This program is one of the most technically complex scientific programs ever undertaken since success is dependent upon developing an unprecedented set of scientific tools to better understand nuclear weapons, enhance stockpile surveillance capabilities, and extend the life of the weapons that comprise the stockpile. Each year, the Secretary of Energy must certify to the President that the weapons are safe and reliable and that underground testing does not need to be resumed.

In meeting the challenges associated with the nuclear weapons stockpile, the Department has had difficulty with the efficiency of its operations, administrative processes, and the ability to conduct timely studies of weapons systems. NNSA management has initiated corrective actions intended to improve management processes over planning and budgeting, information management, acquisitions, and human resources. For example, NNSA has undertaken a major reorganization, initiated in FY 2003, to address some past problems by delineating lines of authority and improving communications.

In our audit of the *National Security Laboratories' Annual Reporting of the Nuclear Weapons Stockpile Assessment* (DOE/IG-0661, September 2004), we found that all three of the laboratories complied with the basic requirements of the *National Defense Authorization Act* when preparing their FY 2003 annual assessment letters to the Secretary. However, we observed that the procedures used by each of the weapons laboratories were somewhat inconsistent in terms of the content and presentation of their assessment letters and in the charters of laboratory technical evaluators who perform independent reviews of the conclusions contained in the assessment reports. In addition, we found that the NNSA Stockpile Coordinator, a Federal official who is the focal point for the critically important assessment program, did not have access to the reports issued by the laboratory technical evaluators.

Our audit of the *Management Controls Over the National Nuclear Security Administration's Enhanced Test Readiness Program* (OAS-M-04-05, August 2004) noted examples of schedule slippages that could potentially impact NNSA's goal to be ready to conduct underground nuclear weapons testing within 18 months. Because the project lacked a number of essential project management tools, including critical components, we could not ascertain, and management could not demonstrate, whether or not the failure to meet these objectives would impact achievement of readiness goals.

Our audit of *The National Nuclear Security Administration's Enhanced Surveillance Campaign* (DOE/IG-0646, April 2004) disclosed that NNSA has experienced delays in completing essential milestones and was at risk of missing some future milestones. The goal of the Enhanced Surveillance Campaign is to provide advance warning of manufacturing and aging defects that could affect the nuclear weapons stockpile. Operating as intended, enhanced surveillance allows NNSA to refurbish weapons before safety, reliability, or performance is impaired.

We also identified project management weaknesses that could impact the stockpile. We reported that the project for the *Reestablishment of Enriched Uranium Operations at the Y-12 National Security Complex*, (DOE/IG-0640, February 2004) will cost substantially more than the planned $119 million. While Y-12 had successfully reestablished three of the key enriched uranium operations processes, several of the remaining processes would not be operational until over 5 years later than originally planned. Completion of the project within technical scope, cost, and

schedule was at risk because the Department had not made full use of available project management controls.

Internal Control Challenges

Internal control challenges relate to the Department's management processes for achieving its missions. Internal control issues, if not addressed, can impede the Department's ability to carry out its program responsibilities and to ensure the integrity of its operations. In this regard, we continue to identify Contract Administration, Project Management, and Information Technology as internal control management challenges facing the Department.

Contract Administration

Effective contract oversight is an essential component for the Department's management of its programs. The Department places a significant reliance on contractors and grantees to accomplish its mission. About three-fourths of the Department's budget is awarded to industrial companies, academic institutions, and nonprofit organizations that operate a broad range of scientific, industrial, and production facilities. Inadequate oversight of contract costs and performance has been a long-standing management issue for the Department. Our reviews in FY 2004 concluded that contract oversight needed to be improved in areas such as claimed costs, purchase cards, and subcontracts.

In our audit of *Central Office Expenses for the Thomas Jefferson National Accelerator Facility* (DOE/IG-0629, December 2003), we concluded that lack of attention by Department administrators to a contractor's claimed costs created an atmosphere in which the contractor sought and received reimbursement for unallowable and inadequately documented central office costs. In that audit, we questioned about $4.6 million of the $4.8 million claimed by and paid to the contractor for central office expenses over a 35-month period. A related investigation resulted in a $1.2 million civil settlement between the Department of Justice and the contractor. Another audit, *Management Controls Over Title X Claims Reimbursement at the West Chicago Thorium Processing Facility*, (OAS-M-04-08, September 2004) disclosed that the contractor had inappropriately claimed about $7 million in non-reimbursable costs, and we questioned $14 million in overhead previously approved by the Department.

Purchase cards have become an effective tool to streamline the procurement process. However, the benefits derived from purchase card use need to be balanced with responsible purchase

card program controls to ensure that Department funds are adequately protected from purchase card abuse. Because of the significance of the issues disclosed through prior examinations, we performed a follow-up review of the *Los Alamos National Laboratory's Purchase Card Program Corrective Actions* (DOE/IG-0644, April 2004) to determine whether the Laboratory had conducted a thorough analysis of its purchase card program and had initiated corrective action to resolve previously reported weaknesses. We found that the Laboratory had significantly improved the management of its purchase card program, but we identified certain opportunities to further reduce the risk of purchase card misuse. In addition, recent reports by the Government Accountability Office found that further improvements were needed to strengthen controls over the purchase card programs at four national laboratories - Lawrence Berkeley, Lawrence Livermore, Pacific Northwest, and Sandia.

The Department's laboratories fulfill their mission by subcontracting a significant portion of their work. We performed a series of audits which identified weaknesses in subcontract administration at national laboratories. Our audit of *Management Controls over Subcontract Administration at the National Security Laboratories* (OAS-M-04-06, August 2004) found that Lawrence Livermore, Los Alamos, and Sandia did not always ensure that audits of subcontractor costs were conducted, questioned costs were resolved, and completed subcontracts were closed timely. Our audit of *Management Controls over Subcontract Administration by the National Renewable Energy Laboratory* (OAS-M-04-02, March 2004) disclosed that the Laboratory did not always adequately protect Government property in the hands of its subcontractors and did not close out subcontracts in a timely manner. Our audit of *Management Controls over Subcontract Administration by the Argonne National Laboratory* (OAS-M-04-01, March 2004) noted that Argonne relied heavily on sole source procurements without, in many cases, adequately supporting their use, and did not always adequately safeguard property acquired by subcontractors.

Other audits identified contract administration weaknesses for property disposal and tuition expenses. In our audit of *Property Disposals at the Yucca Mountain Project* (DOE/IG-0664, September 2004), we concluded that contract administration improvements were needed to ensure that property cleanup and disposal efforts were carried out in a manner designed to maximize the recovery of the Government's investment. For example, we found that the Department received no benefit from property given

to its disposal contractor even though the property had a potential residual value or could be sold as reusable property. Our audit of *Management Controls Over Contractor Tuition Reimbursements for Courses Leading to Degrees at Non-Accredited Educational Institutions* (OAS-M-04-07, September 2004) observed that certain contractors at the Department's Oak Ridge and Richland complexes reimbursed employees for courses and degree programs without ensuring that the institutions offering the courses provided legitimate academic training that would benefit the Department.

In addition, our investigative work in contract administration areas such as labor hour charging, claimed costs, and procurement identified weaknesses and led to recoveries of over $10 million in Federal funds. For example, an investigation led to a civil judgment in the amount of $2.9 million against a former subcontractor and its owner. The investigation determined two subcontractor officials, and their companies, knowingly submitted false claims in the form of coal test reports and invoices. Another investigation determined that a Departmental contractor submitted false purchase orders for payment, mischarged time to a Departmental contract, and billed the Department for personal expenses.

As we reported last year, the Department's Chief Financial Officer, at the request of the Deputy Secretary, has developed a corrective action plan to address five major areas of contract administration: selection of contract type; increasing competition; use of effective performance objectives and measures in contracts; effective management of Departmental activities; and, inadequate human resources to perform contract oversight. In addition, program offices have taken actions to address contractor oversight issues. For example, the Office of Science has initiated an assessment of financial management oversight of its contractors, and the NNSA is structuring its workforce to improve oversight of contractors managing and operating its facilities. Also, the Department's Office of Procurement and Assistance Management has taken a number of additional steps designed to improve the management of contracts.

Project Management

Capital asset and operating projects are an essential component of the Department's missions. The Department's numerous multi-million dollar projects, many unique in the world, support the scientific and technologically complex work of the

Department. In response to criticisms in past years concerning weaknesses in project management, the Department has improved management of capital asset projects.

To address project management issues identified by the Office of Inspector General and other reviewers, such as the National Research Council (an organization of the National Academies of Science engaged by the Department since 1998 to recommend project management improvements), Department leadership initiated a number of corrective actions, particularly for capital asset construction projects. Examples include using external independent reviews to ensure quality planning during early stages of the projects; requiring regular status reports for senior Department management; conducting executive level management reviews; and, implementing a new career development program for project managers. Additionally, Departmental organizations have initiated project management reforms. For example, EM established in its June 2004 *Office of Environmental Management Closure Planning Guidance* that it would identify, plan, and accomplish cleanup activities in accordance with the Department's principles for project management. These projects are valued at over $120 billion in life-cycle costs.

The Office of Inspector General recognizes the Department's progress in this area and acknowledges the sound project management policies and practices established by Department Order DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*, and Manual M 413.3-1, *Project Management for the Acquisition of Capital Assets*. However, in our judgment, programs need to further enhance their efforts by more aggressively applying project management principles to their operating projects and program activities.

During FY 2004, the Office of Inspector General reviewed various on-going projects. For example, in the environmental area, our report on *Major Clean-Up Projects at the Idaho National Engineering and Environmental Laboratory* (DOE/IG-0649, May 2004) recommended that enhancements to contract and project management practices could improve the way the Department and its contractors react to delays and challenges. Because of identified delays, the Department will be forced to deal with additional costs and long-term operational impacts to environmental projects. We also reviewed the WERC Project (a Consortium for Environmental Education and Technology Development) which supports various environmental efforts including education, outreach, research, and student-level design

contests. Our report on the project, *Management Controls Over Administration of the WERC Project* (OAS-M-04-03, May 2004) disclosed that the Department did not ensure that the project was meeting its goals and that reimbursed costs were appropriate.

In our audit of the *Design of the Uranium Storage Facility at the Y-12 National Security Complex* (DOE/IG-0643, March 2004), we concluded that the design for the new facility was unlikely to achieve its intended objectives to provide lower life-cycle costs than the prior design, better security with greater flexibility to adapt to increased security threats, and less risk of construction schedule delays. Our audit of the *Cold Standby Program at the Portsmouth Gaseous Diffusion Plant* (DOE/IG-0634, December 2003) found that the Department had not clearly defined the termination point of the program and total program costs had nearly doubled from initial estimates. In addition, the Department had not formally updated the program mission requirements, assigned program responsibility to a single organization, executed the most cost-effective procurement strategy, or developed a programmatic baseline. In reviewing the *Management of Oak Ridge Radio Transition Projects* (DOE/IG-0653, June 2004), we observed that planned radio transition projects at the Oak Ridge Reservation would cost more than necessary and not provide several critical features, such as enabling protective forces to maintain full communications in the event of an emergency.

Information Technology

Information Technology remains a management challenge as the Department works towards fully implementing the requirements of the *Clinger-Cohen Act of 1996*. To its credit, the Department continues to improve its information technology management. We noted that the Deputy Secretary initiated a campaign to complete certification and accreditation of all major applications and general support systems. In addition, the Department revitalized its Information Technology Council to assist the Chief Information Officer in managing the Department's information technology resources.

The Office of the Chief Information Officer (OCIO) has issued a series of new cyber security policies that address previously reported weaknesses and emphasize a risk-based approach to managing security, that, when implemented, should strengthen cyber security across the Department. The OCIO is also making plans to independently verify and validate the vulnerability

reduction steps being taken. These actions should help ensure that the Department continues to improve its readiness in this important area.

As in past years, a number of Office of Inspector General reports have highlighted internal control weaknesses that impact the improvement of information technology systems and security. For example, in our annual independent evaluation to determine whether the Department's unclassified cyber security program adequately protected data and information systems, *The Department's Unclassified Cyber Security Program - 2004* (DOE/IG-0662, September 2004), we reported that problems continue to exist in the Department's unclassified cyber security program that, if uncorrected, could expose critical systems to compromise. While the number of audit findings was reduced from a high of 69 in FY2002 to 32 in FY 2004, we observed that the Department had not completed implementation of a comprehensive risk management process. The Department's continued difficulty in identifying, tracking, and correcting previously reported weaknesses in a timely manner contributed to remaining cyber security issues.

We also observed in our audit of *Implementation of Indications, Warning, Analysis and Reporting Capability* (DOE/IG-0631, December 2003) that overall cyber security incident reporting had not improved significantly, and sites and organizations continue to have wide discretion in reporting. Without timely and complete incident reporting, the Department's ability to prevent or detect emerging or recurring attacks and to assess cyber security risks is undermined. The OCIO has been successful in significantly improving cyber security incident reporting in the last fiscal year. This was done by issuing a policy that requires both positive and negative reporting, as well as including the status of site reporting in the quarterly Internal President's Management Agenda Scorecard.

In our review of the *Management of the Department's Personnel Security and Access Control Information Systems* (DOE/IG-0651, June 2004), we reported that the Department's information systems modernization initiatives will not adequately address long-standing economy and efficiency issues related to personnel security and physical access systems. The Department's long-term objectives in this area had not developed a comprehensive framework for modernizing these systems and did not always follow sound system development practices. For example, ongoing initiatives will not significantly improve the ability of the Department's

corporate personnel security system to track visitor site access and reduce overlapping or redundant physical access control systems. However, Homeland Security Presidential Directive -12 (HSPD-12) is creating new government-wide standards for identification and access controls, in addition to the ability to track inappropriate attempts to avoid physical and logical security controls. In response to this directive, the OCIO is forming a DOE Task Force to examine how to address the requirements of HSPD-12 in an effective, efficient, and economical manner.

Our audit of the *Management of the Federal Energy Regulatory Commission's Information Technology Program* (DOE/IG-0652, June 2004) noted that the effectiveness of the Commission's information system development activities could have been improved through enhanced project management practices such as developing an enterprise architecture, implementing a capital planning and investment control process, and by thoroughly applying project management techniques. Without improvement, the Commission risks incurring unnecessary costs for systems that face premature obsolescence because they do not meet user needs or satisfy mission requirements. Our audit of *Electricity Transmission Scheduling at the Bonneville Power Administration* (DOE/IG-0637, February 2004) found that Bonneville operated a hybrid system that did not fully meet its needs for scheduling transmission transactions. Specifically, Bonneville's management of the system did not have a comprehensive project plan and lacked system development and implementation procedures. In addition, our audit of *System Development Activities at Selected Management Contractors* (DOE/IG-0647, April 2004) disclosed that Department contractors were not always on track to deliver effective information technology systems on time or at expected cost.

APPENDIX 1

Watch List

Beginning with our prior year's report on management challenges, we developed a watch list that consists of management issues that do not, in our judgment, meet the threshold of major management challenges yet warrant continued attention by senior Department managers. Watch list issues may include management challenges identified in previous years for which the Department has implemented corrective actions or has achieved positive outcomes. The watch list may also include emerging issues that may require Department action. Last year, our watch list addressed three areas: Energy Supply; Worker and Community Safety; and, Performance Management. In our judgment, these three areas remain on the watch list as operational or programmatic functions that need to be closely monitored by Department management.

Energy Supply

One of the critical roles of the Department is to protect our national and economic security by promoting a diverse supply and delivery of reliable, affordable, and environmentally sound energy. In achieving this goal, the Department must confront the disparity between the nation's rising demand for energy and the projected increase in domestic energy supply, as well as address environmental challenges such as greenhouse gas reduction.

The shortfall between energy demand and domestic supply is projected to increase nearly 50 percent by 2020. Consequently, dependence on energy supplied by foreign sources, especially petroleum imports from the Persian Gulf region, will be on the increase as it has been for the past several decades. Acknowledging the trend toward increased dependence on energy supplied by foreign sources, the Administration's National Energy Policy, issued in May 2001, resolved to take steps to improve energy conservation and efficiency and increase domestic energy production in order to avoid increased dependence on imports. The Department promotes energy conservation through programs such as weatherization and building technologies. The Department fosters environmentally-sound domestic energy production by investing in high-risk, high-value energy research and by developing technologies to allow renewable energy to play a more important role in the future of our Nation. These programs include fossil energy, nuclear energy generation, hydrogen programs, and wind technology.

Although, these positive steps are expected to slow the growth in foreign energy dependence, the Department faces the ongoing risk that any serious disruptions in energy supply can impact our security, economy, and standard of living. Disruptions can cause dramatic price fluctuations that reverberate throughout the Nation's economy. A vital component of energy supply is the nation's electric transmission and distribution grid. The ability of this system to function reliably and provide abundant, accessible and affordable electricity is an essential ingredient of the Nation's economy and way of life.

Aging equipment, inadequate transmission capacity in some areas, transmission bottlenecks, and persistent underinvestment in new transmission facilities are impacting the performance of the

grid and its ability to match increasing demand in a digital age. The August 2003 blackout in the Northeast and Midwest demonstrated the serious negative impact that a significant electricity supply disruption can impose, as an estimated 50 million people were affected, with U.S. economic losses estimated to be between $4 and $10 billion.

Given our reliance on foreign energy sources and the significant impact that energy supply disruptions can have on our economy and security, energy supply, in our judgment, is an ongoing issue that needs to be closely watched by Department management.

Worker and Community Safety

Worker and community safety is a high priority of the Department. The large-scale facilities and the dangerous materials that are an integral part of the Department's operations represent safety risks to workers and local communities. Safety incidents have the potential to destabilize, delay, and disrupt the Department's critical activities, and have intangible costs such as a negative public perception of the Department. Prior to FY 2004, we had identified worker and community safety as a major management challenge. Due to progress made and actions initiated, we moved this area to our watch list in FY 2004. We have retained this critical area on our watch list because of the need for the Department to continue to give a high priority to mitigate safety and health risks.

The Office of Inspector General continues to evaluate the Department's safety programs and activities and to make recommendations to assist management in improving its operations. For example, at the request of the Secretary, we performed an investigation of *Allegations Involving Occupational Medical Services and Tank Farm Vapor Exposures at the Hanford Site* (Report I04RL003, June 2004). Although the facts we developed did not substantiate criminal misconduct with regard to the allegations that were the focus of our investigation, we observed several worker health and safety protocols that needed to be addressed by Federal managers at the Hanford site.

In addition, we reviewed the Department's Computerized Accident/Incident Reporting System (CAIRS), which accumulates injury and illness data from facilities throughout the Department complex. Our audit on *The Department's Reporting of Occupational Injuries and Illnesses* (DOE/IG-0648, May 2004), found that CAIRS data for selected contractors was not always accurate or complete as we observed discrepancies between contractor records and CAIRS data and noted that a major contractor was not required to report injury and illness information to the Department. Shortly after issuance of a draft of our report, the Department published the *Environment, Safety and Health Reporting Manual*, which, if fully implemented, should address a number of the data quality concerns identified in our audit.

Performance Management

In FY 2004, due to the considerable progress made by the Department, we no longer identified performance management as a significant management challenge but included it on our watch list of areas that still require management attention. In our judgment, senior Department leadership has acted forcefully to institutionalize performance management as a major driver in

the management of the Department. For example, in FY 2004, the Deputy Secretary directed that internal controls over performance measures be strengthened to ensure, among other things, that performance data are accurate, timely, complete, and adequately supported to permit verification and substantiation of reported results. Nevertheless, since many of the improvements in this area are new and require the continued diligent attention of senior Department management, we retained performance management on our watch list this year.

During FY 2004, the Office of Inspector General continued to assist in the evaluation of performance measures to assure accurate and valid results are reported and documented against clear and meaningful measures. In a report on the *Federal Energy Regulatory Commission's Performance Management* (DOE/IG-0627, November 2003), we observed that, while many of the Commission's performance measures were appropriate, the performance management system did not reach its full potential. For example, a few key activities did not have measures, measures did not always address program activities, and, in some cases, management could not demonstrate that it had actually achieved reported results.

In our report on *The Department's Audit Resolution Process* (DOE/IG-0639, February 2004), we noted that, although the Department had made efforts to improve the effectiveness of its audit resolution process, there were several areas where additional action was necessary. Lack of specific, quantifiable performance measures diminished the overall effectiveness of the Department's audit resolution process and Department organizations had not been required to perform trend analyses to identify systemic problems or review audit findings issued to others for applicability. Consequently, the Department had not always realized potential programmatic savings, improvements in health and safety, and operational efficiencies that could be achieved through a strong audit resolution process.

Appendix 2

TABLE COMPARING MANAGEMENT CHALLENGES REPORTED BY VARIOUS GROUPS

IG	GAO[1]	DOE[2]
Environmental Cleanup	Cleanup of Radioactive & Hazardous Waste	Environmental Cleanup
		Nuclear Waste Disposal
National Security	Security Threats and Problems	Security
Stockpile Stewardship	Nuclear Weapons Stockpile	Stockpile Stewardship
Contract Administration	Contract Management	Oversight of Contractors
Project Management		Project Management
Information Technology Management		Information Technology Management
		Safety and Health
		Human Capital Management
	Revitalize Infrastructure	
	Leadership in Meeting Nation's Energy Needs	

[1]According to *Major Management Challenges and Program Risks, Department of Energy* (GAO-03-100, January 2003)

[2]DOE's self identified "Significant Issues" according to *U.S. Department of Energy Performance and Accountability Report, Fiscal Year 2004* (November 2004)

Appendix 3

RELATED REPORTS ISSUED IN FISCAL YEAR 2004

National Security

- Inspection Report on *Reporting of Security Incidents at the Lawrence Livermore National Laboratory* (DOE/IG-0625, November 4, 2003)
- Inspection Report on *Internal Controls Over Classified Computers and Classified Removable Media at the Lawrence Livermore National Laboratory* (DOE/IG-0628, December 5, 2003)
- Audit Report on *Safeguards Over Sensitive Technology* (DOE/IG-0635, January 13, 2004)
- Inspection Report on *Protective Force Performance Test Improprieties* (DOE/IG-0636, January 23, 2004)
- Audit Report on *Recovery of Highly Enriched Uranium Provided to Foreign Countries* (DOE/IG-0638, February 9, 2004)
- Audit Report on *The Department's Basic Protective Force Training Program* (DOE/IG-0641, March 12, 2004)
- Inspection Report on *Contractor Compliance with Deemed Export Controls* (DOE/IG-0645, April 13, 2004)
- Inspection Report on *Unauthorized Handguns on National Nuclear Security Administration Aircraft* (DOE/IG-0654, July 6, 2004)
- Inspection Report on *Internal Controls Over Personal Computers at Los Alamos National Laboratory* (DOE/IG-0656, August 10, 2004)
- Audit Report on *The Department's Continuity Planning and Emergency Preparedness* (DOE/IG-0657, August 11, 2004)
- Inspection Report on *Protective Force Response to a Security Incident at Sandia National Laboratory, California* (DOE/IG-0658, August 11, 2004)
- Inspection Report on *Internal Controls Over the Accountability of Computers at Sandia National Laboratory, New Mexico* (DOE/IG-0660, August 30, 2004)
- Inspection Report on *Intelligence Oversight Activities at Selected Field Sites* (INS-O-04-01, August 31, 2004)

- Inspection Report on *Control and Accountability of Emergency Communication Network Equipment* (DOE/IG-0663, September 24, 2004)

Environmental Cleanup

- Audit Report on *Reindustrialization of the East Tennessee Technology Park* (DOE/IG-0623, October 14, 2003)
- Audit Report on *Transuranic Waste Retrieval and Processing at the Hanford Site* (DOE/IG-0624, October 23, 2003)
- Audit Report on *Depleted Uranium Hexafluoride Conversion* (DOE/IG-0642, March 18, 2004)
- Audit Report on *Management Controls Over the Licensing Support Network for the Yucca Mountain Repository* (OAS-M-04-04, May 20, 2004)
- Audit Report on *Groundwater Remediation Activities at Hanford* (DOE/IG-0655, July 22, 2004)
- Audit Report on *The Stabilization of Nuclear Materials at Los Alamos National Laboratory* (DOE/IG-0659, August 16, 2004)

Stockpile Stewardship

- Audit Report on *Modernization of Tritium Requirements Systems* (DOE/IG-0632, December 16, 2003)
- Audit Report on *Reestablishment of Enriched Uranium Operations at the Y-12 National Security Complex* (DOE/IG-0640, February 24, 2004)
- Audit Report on *The National Nuclear Security Administration's Enhanced Surveillance Campaign* (DOE/IG-0646, April 14, 2004)
- Audit Report on *Management Controls Over the National Nuclear Security Administration's Enhanced Test Readiness Program* (OAS-M-04-05, August 3, 2004)
- Audit Report on *National Security Laboratories' Annual Reporting of the Nuclear Weapons Stockpile Assessment* (DOE/IG-0661, September 14, 2004)

Contract Administration

- Audit Report on *Central Office Expenses for the Thomas Jefferson National Accelerator Facility* (DOE/IG-0629, December 8, 2003)

- Audit Report on *Management Controls over Subcontract Administration by the Argonne National Laboratory* (OAS-M-04-01, March 12, 2004)

- Audit Report on *Management Controls over Subcontract Administration by the National Renewable Energy Laboratory* (OAS-M-04-02, March 19, 2004)

- Special Report on *Los Alamos National Laboratory's Purchase Card Program Corrective Actions* (DOE/IG-0644, April 12, 2004)

- Audit Report on *Management Controls over Subcontract Administration at the National Security Laboratories* (OAS-M-04-06, August 19, 2004)

- Audit Report on *Management Controls Over Contractor Tuition Reimbursements for Courses Leading to Degrees at Non-Accredited Educational Institutions* (OAS-M-04-07, September 22, 2004)

- Audit Report on *Management Controls Over Title X Claims Reimbursement at the West Chicago Thorium Processing Facility*, (OAS-M-04-08, September 24, 2004)

- *Property Disposals at the Yucca Mountain Project* (DOE/IG-0664, September 27, 2004)

Project Management

- Audit Report on *The McNeil Biomass Project* (DOE/IG-0630, December 11, 2003)

- Audit Report on *Cold Standby Program at the Portsmouth Gaseous Diffusion Plant* (DOE/IG-0634, December 22, 2003)

- Audit Report on *Design of the Uranium Storage Facility at the Y-12 National Security Complex* (DOE/IG-0643, March 19, 2004)

- Audit Report on *Management Controls Over Administration of the WERC Project* (OAS-M-04-03, May 18, 2004)

- Audit Report on *Major Clean-Up Projects at the Idaho National Engineering and Environmental Laboratory* (DOE/IG-0649, May 25, 2004)

- Audit Report on *Management of Oak Ridge Radio Transition Projects* (DOE/IG-0653, June 30, 2004)

Information Technology

- Audit Report on *Implementation of Indications, Warning, Analysis and Reporting Capability* (DOE/IG-0631, December 12, 2003)

- Audit Report on *Electricity Transmission Scheduling at the Bonneville Power Administration* (DOE/IG-0637, February 4, 2004)

- Audit Report on *System Development Activities at Selected Management Contractors* (DOE/IG-0647, April 22, 2004)

- Audit Report on *Management of the Department's Personnel Security and Access Control Information Systems* (DOE/IG-0651, June 18, 2004)

- Audit Report on *Management of the Federal Energy Regulatory Commission's Information Technology Program* (DOE/IG-0652, June 30, 2004)

- Evaluation Report on *The Department's Unclassified Cyber Security Program - 2004* (DOE/IG-0662, September 24, 2004)

Worker and Community Safety

- Audit Report on *The Department's Reporting of Occupational Injuries and Illnesses (CAIRS)* (DOE/IG-0648, May 21, 2004)

- Investigation of *Allegations Involving Occupational Medical Services and Tank Farm Vapor Exposures at the Hanford Site* (I04RL003, June 1, 2004)

- Inspection Report on *Internal Controls Over Methamphetamine Precursor Chemicals at the Y-12 National Security Complex and the Oak Ridge National Laboratory* (DOE/IG-0650, June 14, 2004)

Performance Management

- Audit Report on *Federal Energy Regulatory Commission's Performance Management* (DOE/IG-0627, November 24, 2003)

- Audit Report on *The Department's Audit Resolution Process* (DOE/IG-0639, February 17, 2004)

IG Report No. DOE/IG-0667

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

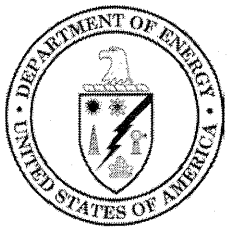
If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

13



U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory

DOE/IG-0677

February 2005

Department of Energy

Washington, DC 20585

February 22, 2005

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory"

BACKGROUND

Los Alamos National Laboratory (LANL), as part of the National Nuclear Security Administration (NNSA), contributes to meeting the Nation's nuclear deterrence capability and other security needs. LANL is operated by the University of California (UC) and is one of the Department of Energy's most sensitive sites. The laboratory directly employs about 7,500 UC employees, of which approximately 800 terminate their employment each year.

During previous reviews by the Office of Inspector General, concerns were raised about the adequacy of internal controls over property at LANL. Therefore, the objective of our inspection was to determine the adequacy of LANL internal controls for management to ensure that terminating employees accounted for Government property at the time of their departure. To achieve this objective, we sampled transactions related to LANL employee out-processing; reviewed related documents, including LANL procedural directives; and interviewed responsible contractor and Federal officials.

RESULTS OF INSPECTION

LANL out-processing procedures were not followed by more than 40 percent of the 305 terminating employees included in our sample. Consequently, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating. Given this and the results of additional sampling, we found that there was no assurance that, prior to departure, LANL terminating employees turned in security badges, completed the required Security Termination Statement, or had their security clearances and access authorizations to classified matter and/or special nuclear material terminated in a timely manner. To illustrate, of a sample of 96 cleared employees who departed LANL over a 2-year period:

- Forty-four employees had not turned in their badges at the time of our field work;
- Sixty-one employees did not complete the Security Termination Statement at the time of their departure;
- Twenty-one employees retained their clearances in the Department's official database from 11 to 567 days after their departure; and

Printed with soy ink on recycled paper

- One employee retained his sensitive compartmented information access authorization for more than 5 months after his retirement.

Further, we found that there was no assurance that, prior to departure, LANL terminating employees:

- Accounted for classified holdings, such as documents and classified removable electronic media (CREM), and personal property, such as computers and laboratory equipment. However, our limited checks did not identify any unaccounted for items assigned to terminated employees; and

- Cleared the LANL Payroll Team for the purpose of stopping wage payments and addressing outstanding financial obligations.

Subsequent to completion of our fieldwork, LANL revised its out-processing procedures to address some of the concerns we raised during the inspection. The revised procedures were not in place long enough for us to assess their effectiveness. However, we noted that the revised procedures (1) transferred responsibility for out-processing from the terminating employee to the applicable Line Manager and (2) were expanded to specifically include the collection, return, and reassignment of CREM.

We made several recommendations to the Manager of the Los Alamos Site Office that were designed to enhance safeguards and security and property controls at LANL.

MANAGEMENT REACTION

In responding to a draft of this report, NNSA generally agreed with the report and corresponding recommendations and indicated that corrective actions have been implemented. However, NNSA disagreed with our characterization of the seriousness of the consequences resulting from the lack of adherence to established out-processing procedures. NNSA believed it was "more accurate to state there is potential for unauthorized access."

In general, management's comments were responsive to our findings and recommendations. However, it is clear that a key premise of the Department's security program is that only authorized persons have access to classified and sensitive facilities and/or information. Thus, we believe that the issues described in our report must be considered serious, especially in the present environment.

Management's comments are provided in their entirety in Appendix B of the report.

Attachment

cc: Administrator, National Nuclear Security Administration
Director, Office of Security and Safety Performance Assurance
Director, Policy and Internal Controls Management
Director, Office of Program Liaison and Financial Analysis

SECURITY AND OTHER ISSUES RELATED TO OUT-PROCESSING OF EMPLOYEES AT LOS ALAMOS NATIONAL LABORATORY

TABLE OF CONTENTS

OVERVIEW

Introduction and Objectives 1

Observations and Conclusions 1

DETAILS OF FINDINGS

Out-Processing Procedures 3

Performance Measures 8

RECOMMENDATIONS 8

MANAGEMENT COMMENTS 9

INSPECTOR COMMENTS 9

APPENDICES

A. Scope and Methodology 10

B. Management Comments 11

Overview

INTRODUCTION AND OBJECTIVES

The core mission of the Department of Energy's (DOE's) Los Alamos National Laboratory (LANL) is to enhance global security, develop technical solutions to reduce the weapons of mass destruction threat, and improve the cold war environmental and nuclear materials legacy. Given its national security mission, LANL is one of DOE's most sensitive sites. LANL is operated by the University of California (UC) and administered by the National Nuclear Security Administration (NNSA). It directly employs approximately 7,500 UC employees. Approximately 800 UC employees terminate employment at LANL annually.

During previous reviews by the Office of Inspector General, concerns were raised about the adequacy of internal controls over property at LANL. Further, during a February 26, 2003, congressional hearing before the House Energy and Commerce Committee's Subcommittee on Oversight and Investigations, a former LANL employee testified that retiring employees took Government property with them when they left the laboratory.

Based upon this, the objective of our inspection was to determine the adequacy of LANL internal controls for management to ensure that terminating employees accounted for Government property at the time of their departure. To achieve this objective, we conducted several samples of transactions related to LANL employee out-processing; reviewed related documents, including LANL procedural directives; and interviewed numerous responsible contractor and Federal officials.

OBSERVATIONS AND CONCLUSIONS

More than 40 percent of the 305 cleared and uncleared terminating employees included in our sample did not follow LANL out-processing procedures. Consequently, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating. Given this and the results of additional sampling, we concluded that the process did not provide assurance that, prior to departure, LANL terminating employees:

- Turned in security badges, received the required Security Termination Briefing, completed the required Security Termination Statement, or had their security clearances and access authorizations to classified matter and/or special nuclear material terminated in a timely manner. For example, of a sample of 96 cleared employees who departed LANL over a 2-year period: 44 employees did not turn in their badges; 61

employees did not complete the Security Termination Statement at the time of their departure; 21 employees retained their clearances in DOE's official database anywhere from 11 to 567 days after departure; and 1 employee retained his sensitive compartmented information (SCI) access authorization for more than 5 months after his retirement.

- Accounted for classified holdings, such as documents and classified removable electronic media (CREM), and personal property, such as computers and laboratory equipment. However, a limited review of personal property that had been assigned to terminated employees did not identify any unaccounted for items.

- Cleared the LANL Payroll Team for the purpose of stopping wage payments and addressing outstanding financial obligations.

We found that the contract between the Department and LANL did not contain performance measures to evaluate the effectiveness of the LANL employee out-processing procedures. We believe such a mechanism is important since LANL's termination process is intended, in part, to account for classified and unclassified Government property.

On September 14, 2004, subsequent to completion of our fieldwork, LANL revised its out-processing procedures to address some of the concerns we raised during this inspection. The revised procedures have not been in place long enough for us to assess their effectiveness. However, under the revised procedures, the responsibility for out-processing has been transferred from the terminating employee to the applicable Line Manager (i.e., Group Leader or above). We also noted that the revised procedures were expanded to specifically include the collection, return, and reassignment of CREM. We believe that the Department should ensure that LANL incorporates recommended corrective actions associated with the internal control weaknesses identified in this report as it implements the new out-processing procedures.

This inspection expands upon work performed by the Office of Inspector General at several DOE sites, which is discussed in an audit report entitled "Personnel Security Clearances and Badge Access Controls at Selected Field Locations" (DOE/IG-0582, January 2003). The audit found that, among other things, a number of employees departed LANL without surrendering their badges; however, only a few retained authority to access sensitive areas or classified material.

Details of Findings

OUT-PROCESSING PROCEDURES

We found that more than 40 percent of the 305 terminating employees in our sample did not follow LANL out-processing procedures. As a result, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating, and key elements of the out-processing procedures were not performed timely. The out-processing procedures were outlined on the LANL internal web site at the Human Resources (HR) Homepage. Terminating employees were required to download a Departure Processing form or obtain it from the Division HR representative or the HR Division office and out process with applicable LANL organizations.

Using the Departure Processing form, regular LANL employees were required to obtain the signatures of the individuals responsible for 14 key elements of the termination process. Student employees (i.e., those who have completed high school, been accepted in an undergraduate program or above, and received 90-day to 1-year appointments) were required to obtain the signatures of the individuals responsible for 8 key elements of the termination process. Some of the signatures included on the Departure Processing forms are those of Property Administrators, Document Custodians, Key Custodians, Librarians, Benefits Specialists, and Badge Office personnel. Their signatures were intended to document that personal property, classified holdings, keys, and badges were accounted for prior to an employee's departure and that security clearances and access authorizations (i.e., authorizations to access classified matter or special nuclear material) were properly terminated.

Reviewing a judgmental sample of 305 employees out of 1,668 employees who terminated between January 1, 2002, and February 25, 2004, we identified that 129 of the associated HR files were missing the Departure Processing form. In most instances, it did not appear that HR had formal advance notice that these 129 employees were leaving the laboratory. As HR became aware of these departures, it notified the following LANL organizations: Security, Travel, Smart Cards (these cards allow access to the LANL intranet), Benefits, Property Administration, and Payroll. This notification was made using an HR Terminations Memorandum, which referred to the problem identified during this review by stating, "This is to assist your organization since this employee did not complete the departure process."

The HR memorandum was the first written notification of departure to affected organizations. However, we determined that the HR memoranda were often issued more than a week after an employee left the laboratory.

As a result of termination notification delays, supporting organizations frequently did not accomplish out-processing tasks prior to an employee's departure. This had what were, in our judgment, significant consequences, which are described in the following portions of this report.

Security Badges

The process did not provide assurance that all terminating employees turned in their security badges prior to departure. Since the Departure Processing form was not always used, the LANL Security and Safeguards Division, which is responsible for the collection of badges, frequently was not provided advance notice about terminating employees. As a result, 162 of the 1,668 employees who terminated between January 1, 2002, and February 25, 2004, or approximately 10 percent, did not turn in their badges prior to departure. These included employees with the following types of badges:

- 33 Q-cleared badges, which allow access up to top secret information and specified quantities and types of special nuclear material;

- 11 L-cleared badges, which allow access up to secret information and smaller quantities and types of special nuclear material; and

- 118 uncleared badges, which allow access to LANL unclassified facilities and areas.

At the time of our fieldwork, entrance to certain LANL facilities was controlled through manual badge checks by security officers, not electronic means. Also, under certain circumstances, LANL badges allowed access to other DOE facilities. Therefore, a terminated employee who had retained his/her badge could potentially access laboratory facilities and classified information and materials, as well as other DOE sites. However, there was no practical way to readily determine if such access had, in fact, occurred given circumstances such as the existence of LANL entrance points that relied on manual badge checks.

Security Clearances and Access

There was no assurance that terminating employees received the required Security Termination Briefing, completed the required Security Termination Statement, or had their security clearances and access authorizations terminated in a timely manner. The retention of security clearances combined with the retention of badges by terminated employees increases the potential for terminated employees to obtain unauthorized access to facilities and/or classified information after departure.

DOE Manual (M) 470.1-1, "Safeguards and Security Awareness Program," states that a Security Termination Briefing is required whenever access authorization has been or will be terminated. Security Termination Briefings are used to impress upon the individual his or her continuing responsibility not to disclose classified information. This briefing also addresses the individual's obligation to return to appropriate DOE officials all classified documents and materials in the individual's possession prior to departure.

After the Security Termination Briefing, the terminating employee and the Security Specialist who conducted the briefing sign DOE Form (F) 5631.29, "Security Termination Statement." This form is used by LANL to provide the required notification to the cognizant DOE Personnel Security Office of the termination of an employee. Based on this form, the DOE Personnel Security Office terminates the employee's security clearance and access authorization in DOE's Central Personnel Clearance Index (CPCI) system.

We sampled 96 DOE Q-cleared and L-cleared employees who departed the laboratory during the period January 1, 2002, to February 25, 2004, 44 of whom had not turned in their badges. Of the 96 employees, we identified 61 employees who did not complete the Security Termination Statement at the time of their departure. As a result, some security clearances were not terminated in the CPCI system in a timely manner. Specifically, 21 of the 61 Q-cleared and L-cleared employees who did not complete the Security Termination Statement retained their clearances in the CPCI anywhere from 11 to 567 days after their departure. Further, of the 21 employees, 6 had not turned in their security badges at the time of their departure from the laboratory.

We found that the cognizant DOE Personnel Security Office was unaware that 3 of the 21 employees had terminated from the laboratory. The 3 employees retained active clearances ranging from 377 days to 567 days following their respective terminations.

The Office of Inspector General immediately notified the DOE Personnel Security Office of our concern, and we confirmed that action was taken to terminate the clearances. Among the other departed employees, we found that four employees had clearances that were active for periods ranging from approximately three months to nine months after termination.

We followed up to determine whether any of the 96 departed employees had SCI access authorization and, if so, whether that authorization was terminated timely. We determined that five of the departed employees had SCI access authorization through LANL and that one of those employees retained his SCI access authorization for five months after retiring from LANL. We interviewed this former employee, and he told us that a few months after his retirement he took a position with a LANL subcontractor. He advised us that he was unaware of any need for the retention of his SCI access authorization after he retired from LANL and did not recall accessing any SCI material after his retirement. In addition, an official with the subcontractor told us that an SCI access authorization was not required as a condition of the individual's employment.

Classified Holdings

There was no assurance that terminating employees accounted for classified holdings prior to departure. Although our limited checks did not identify any unaccounted for classified holdings assigned to terminated employees, we noted that Document Custodians often did not have the opportunity to reconcile classified holdings with these employees. We believe this increases the potential for unaccounted for classified holdings to be identified after an employee has departed and is unavailable to assist with reconciliation.

It was the responsibility of the terminating employee and the associated Document Custodian to clear the employee's accounts of all classified holdings. Since the Departure Processing form was not always used, Document Custodians responsible for the accountability of classified holdings were frequently unaware that employees who reasonably would be expected to have classified holdings were departing the laboratory. We also determined that although students may have authorized access to classified materials, the Departure Processing for Students form did not include a signature line for the Document Custodian.

Of even greater concern, the out-processing procedures did not address the accountability of CREM when employees responsible

for the control of this material departed the laboratory. Specifically, we determined that the Departure Processing forms for both regular employees and students did not contain a specific out-processing signature line for CREM Custodians. As noted previously, LANL's revised out-processing procedures were expanded to include the collection, return, and reassignment of CREM. Since LANL has experienced significant problems in the control and accountability of this material in the past, we believe that LANL should place special emphasis on the accountability of CREM during the implementation of the revised out-processing procedures.

Personal Property

There was no assurance that terminating employees accounted for personal property, such as computers and laboratory equipment, prior to departure. It was the responsibility of the terminating employee and the Property Administrator to account for all LANL equipment and property before an employee departed. These activities included determining what property items were affected, locating these items, obtaining reassignment guidance from management, reassigning the items, and performing database entries.

Since the Departure Processing form was not always used, Property Administrators were frequently unaware that employees were departing the laboratory. Although our limited review did not identify any unaccounted for property assigned to terminated employees, Property Administrators frequently had to complete required termination activities after employees left the laboratory. We believe this increases the potential for unaccounted for property to be identified after an employee's termination, which diminishes LANL's ability to hold employees accountable for assigned property.

Financial Clearance

There was no assurance prior to their departure that terminating employees cleared the LANL Payroll Team for the purpose of stopping wage payments and addressing outstanding financial obligations. The Payroll Team was frequently unaware that employees departed the laboratory. We found instances where this resulted in overpayments and unresolved obligations. For example, one employee was paid for an additional week's salary after his designated termination date, and four employees departed the laboratory owing for advanced leave.

PERFORMANCE MEASURES

We found that there was no mechanism identified under the LANL performance objectives and measures to evaluate the effectiveness of the HR termination process.

Our review of the contractor performance objectives and measures for Fiscal Year (FY) 2004 determined that the LANL contract, Appendix F, contained a performance objective that addressed the effectiveness of internal controls associated with LANL HR business systems. The performance objective stated "Improve or maintain effective business systems and practices that safeguard public assets and support mission objectives."

The "LANL Implementation Guidelines for FY04 Appendix F, Performance Objectives and Measures" developed by the laboratory contained the evaluation basis for determining the laboratory's performance. The performance measure in this document that correlates with the above performance objective stated "Demonstrate effective internal business controls and processes to maintain an acceptable . . . Human Resources administrative systems . . . ." However, the evaluation basis only addressed five HR processes: new hires, student hires, position classification, start salaries, and promotional increases. The LANL evaluation basis did not address the HR termination process. We believe such a mechanism is important since LANL's termination process is intended, in part, to account for classified and unclassified Government property.

RECOMMENDATIONS

We recommend that the Manager, Los Alamos Site Office, ensures that:

1. LANL's revised out-processing procedures adequately address the issues identified in this report and are being appropriately implemented.

2. LANL conducts a review of terminated employees who retained their badges and/or access authorizations after their official termination dates to determine if they obtained unauthorized access to DOE facilities and/or classified holdings.

3. LANL conducts a review of all employees who terminated without following the appropriate out-processing procedures to ensure that any CREM or classified holdings assigned to these employees have been properly accounted for.

4. LANL recovers badges of terminating employees, conducts Security Termination Briefings, completes Security Termination Statements, and makes timely notification to DOE when security clearances and access authorizations should be terminated.

5. Prior to the departure of terminating employees, LANL accounts for all Government property assigned to the employees, to include personal property, classified holdings, and CREM.

6. Prior to the departure of terminating employees, LANL reconciles outstanding financial obligations.

7. LANL's implementation guidelines for its performance objectives and measures are revised to include an evaluation of the HR termination process as part of the overall evaluation of the HR administrative system.

MANAGEMENT COMMENTS

In comments on our draft report, management generally agreed with our report and recommendations and indicated that corrective actions have been taken or initiated. However, NNSA disagreed with our characterization of the seriousness of the consequences resulting from the lack of adherence to established out-processing procedures, and NNSA believed it was "more accurate to state there is potential for unauthorized access." Management also provided two comments about specific phrasing in the report.

INSPECTOR COMMENTS

We found management's comments to be generally responsive to our report. However, we disagree with NNSA's position regarding the seriousness of the issues raised in this report. The integrity of the Department's security program is built on the premise that only authorized persons have access to classified and sensitive information.

Regarding management's two comments concerning specific phrasing in the report, we evaluated the matter and made appropriate changes.

Appendix A

SCOPE AND METHODOLOGY

We conducted our inspection fieldwork between January and August 2004. We interviewed laboratory officials regarding LANL out-processing procedures and reviewed DOE and LANL policies, procedures, and records regarding employee terminations, security clearance and access authorization terminations, personal property, badges, classified holdings, and payroll. We also interviewed DOE officials regarding security clearance and access authorization terminations, property accountability, and performance measures. Documents of primary interest were:

- DOE M 470.1-1, "Safeguards and Security Awareness Program."
- DOE O 472.1C, "Personnel Security Activities."
- DOE M 472.1-1B, "Personnel Security Program Manual."
- DOE M 473.1-1, "Physical Protection Program Manual."
- LANL Property Management Manual.

Also, pursuant to the "Government Performance and Results Act of 1993," we reviewed LANL's performance measurement processes as they relate to HR business systems.

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

February 10, 2005

MEMORANDUM FOR Alfred K. Walter
Assistant Inspector General
for Inspections and Special Inquiries

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Revised Comments to Draft Inspection Report on Employee Out-Processing at LANL

The National Nuclear Security Administration (NNSA) appreciates the opportunity to have reviewed the Inspector General's (IG) draft inspection report, S04IS008, "Out-Processing of Employees at Los Alamos National Laboratory." We understand that this inspection was the result of Congressional testimony by a former Laboratory employee who claimed that retiring employees took Government property with them when they, the employees, left the Laboratory.

Generally, NNSA agrees with the report and corresponding recommendations. In fact corrective actions were implemented and completed prior to the issuance of the draft report. While we agree with the report we are providing the following comments.

- Observations and Conclusions; page one, paragraph four - talks to personnel being frequently unaware that employees had left the laboratory. It would be more correct to reflect the lack of timeliness of notifications since all of the administrative offices mention were notified, albeit after the employees left and through memoranda.

- Page four, first paragraph talking about security badges - it is more accurate to state that "in 10% of the cases, there was no assurance...." rather than stating that there was no assurance that terminating employees turned in their security badges when the report also states 90% of departing employees did turn in badges upon termination.

- NNSA disagrees with the IG's contention of "serious consequences" as stated in the report. We do believe that, left uncorrected, it is more accurate to state there is "potential for unauthorized access."

Printed with soy ink on recycled paper

Should you have any questions about this response, please contact Richard Speidel, Director, Policy and Internal Controls Management. He may be contacted at 202-586-5009.

Attachment

cc: Robert Braden, Senior Procurement Executive
Edwin Wilmot, Manager, Los Alamos Site Office
Karen Boardman, Director, Service Center

Comments to Recommendations
Draft Inspection Report, S04IS008
"Out-Processing of Employees
at Los Alamos National Laboratory"

The following are specific comments to the recommendations.

We recommend that the Manager, Los Alamos Site Office, ensures that:

Recommendation 1

LANL's revised out-processing procedures adequately address the issues identified in this report and are being appropriately implemented.

Management Comment

Concur

Action Complete. The out-processing procedures that the Laboratory revised address the issues raised in the report and the procedures have been implemented.

Recommendation 2

LANL conducts a review of terminated employees who retained their badges and/or access authorizations after their official termination dates to determine if they obtained unauthorized access to DOE facilities and/or classified holdings.

Management Comment

Concur With Intent

NNSA agrees with the intent of the recommendation. However, we do not agree with the implementation of the recommendation the way it is worded. For the Laboratory to conduct a review of terminated employees would be cost prohibited and resource intensive. Additionally, those employees that have terminated employment that did not have clearances could easily return to the property (open) areas of the Laboratory justifiably and without the knowledge of Laboratory management. However, for those employees that have terminated employment and that held clearances/access authorizations, they are prohibited from entering protected areas. Security measures are such that they prevent this type of

unauthorized access. There is an established process whereby changes are made to an employee's status from active to inactive when employment terminates, and this automatically prevents access to security areas via electronic means. There are four data points that are electronically verified when an individual swipes his or her badge to access a security area, including: (1) an active employee record; (2) an active security badge; (3) a current security refresher briefing record; and, (4) an active clearance. Even in those cases where an employees' security badge was not retrieved access to the security areas is not possible. NNSA believes that with the implementation of all of the other recommendations, the concerns raised by this recommendation will be addressed. However, the Site Office will pursue opportunities with the Laboratory for the Laboratory to conduct a random sampling of terminated employees who possessed clearances/access authorizations to determine if any of those terminated employees tried to access protected areas after their termination.

Recommendation 3

LANL conducts a review of all employees who terminated without following the appropriate out-processing procedures to ensure that any CREM, or classified holdings assigned to these employees has been properly accounted for.

Management Comment

Concur

Action Complete. A 100% wall-to-wall inventory of accountable CREM in complete. All documents are accounted for. Therefore, there is not an issue related to missing CREM and employees that did not properly out-process when terminating employment.

Recommendation 4

LANL recovers badges of terminating employees, conducts Security Termination Briefings, completes Security Termination Statements, and makes timely notification to DOE when security clearances and access authorizations should be terminated.

Management Comment

Concur

Action Complete. As part of the implemented, revised out-processing procedures, terminating employees go through one or all of the following: collection of terminating employee badges; conduct of Security Termination Briefings; completion of Security Termination Statements; and notification when security clearances and access authorizations must be terminated.

Recommendation 5

Prior to the departure of terminating employees, LANL accounts for all Government property assigned to the employees, to include personal property, classified holdings, and CREM.

Management Comment

Concur

Action Complete. Revised procedures account for government property, CREM, and/or classified holdings related to individuals terminating employment.

Recommendation 6

Prior to the departure of terminating employees, LANL reconciles outstanding financial obligations.

Management Comment

Concur

Action Complete. Any financial obligations are resolved to the extent allowed by law and/or is financially beneficial to the Laboratory.

Recommendation 7

LANL's implementation guidelines for its performance objectives and measures are revised to include an evaluation of the HR termination process as part of the overall evaluation of the HR administrative system.

Management Comment

Concur

4

The Site Office Manager has directed that, for FY 2005, an Appendix F measure be developed to include "safe and secure departure of all employees should account for many items including, but not limited to, LANL property, LANL badges, clearance processing, and financial stewardship. At least 97.5% of terminating employees will be properly exited according to the encompassing and newly implemented departure process.

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message clearer to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

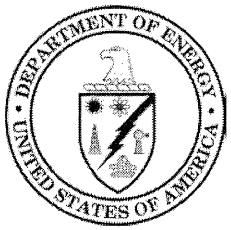
If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

14



U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Security Access Controls at the Y-12 National Security Complex

DOE/IG-0691 June 2005

Department of Energy
Washington, DC 20585

June 14, 2005

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Security Access Controls at the Y-12 National Security Complex"

BACKGROUND

The Office of Inspector General received information that non-U.S. citizens were improperly allowed access to a leased facility at the Department of Energy's Y-12 complex in Oak Ridge, Tennessee. Y-12, part of the National Nuclear Security Administration (NNSA), is designated as a National Security Complex and is one of the Department's most sensitive sites. We initiated an inspection to evaluate the factual basis of the allegation and, if confirmed, to determine whether control procedures at Y-12 should have prevented such access.

RESULTS OF INSPECTION

We found that foreign construction workers, using false documents, had, in fact, gained access to the Y-12 site on multiple occasions. Specifically, 16 foreign construction workers were found to have been illegal aliens. Some of these workers acquired facility access badges and were, as a result, permitted access to the main Y-12 site. Others were able to access an adjacent Y-12 leased facility.

Further, certain information associated with the construction of the Y-12 leased facility, which was planned to store documents classified up to Secret-Restricted Data, was considered Unclassified Controlled Nuclear Information and Official Use Only. While this was a significant concern, we did not uncover any evidence that such information was compromised.

Finally, we determined that access control procedures at Y-12, which might have prevented unauthorized access, either were not implemented or were not effective. These are more fully described in the report, but included reliance on construction subcontractors to self-certify as to the status of their workers.

When informed of our findings, Y-12 management took prompt corrective action. However, we are concerned that process shortcomings similar to those found at Y-12 may exist at other Department of Energy locations. Therefore, we are recommending

Printed with soy ink on recycled paper

that the Office of Independent Oversight and Performance Assurance (OA) augment its security review processes to address these issues.

MANAGEMENT REACTION

Management concurred in our findings and recommendations and committed to taking necessary corrective actions. NNSA, for example, stated that it would make all of its site office managers aware of the findings at Y-12 to ensure that steps are taken, if necessary, to improve facility access controls. The Office of Security and Safety Performance Assurance, OA's parent organization, informed us that access controls have been a recognized weakness across the Government and that much work is being done to prevent reoccurrences of the types of issues identified in this report.

Attachment

cc: Deputy Secretary
Chief of Staff
Administrator, National Nuclear Security Administration
Director, Office of Security and Safety Performance Assurance
Director, Office of Independent Oversight and Performance Assurance
Manager, Y-12 Site Office
Director, Office of Program Liaison and Financial Analysis (ME-100)
Director, Policy and Internal Controls Management (NA-66)

SECURITY ACCESS CONTROLS AT THE Y-12 NATIONAL SECURITY COMPLEX

TABLE OF CONTENTS

OVERVIEW

Introduction and Objective 1

Observations and Conclusions 1

DETAILS OF FINDINGS

Access to Y-12 by Non-U.S. Citizens 2

Lessons Learned 3

RECOMMENDATIONS 3

MANAGEMENT COMMENTS 3

INSPECTOR COMMENTS 4

APPENDICES

A. Scope and Methodology 5

B. Management Comments 6

Overview

INTRODUCTION AND OBJECTIVE

The Department of Energy's (DOE) Y-12 National Security Complex (Y-12) in Oak Ridge, Tennessee, is a component of the National Nuclear Security Administration and is an integral part of the nuclear weapons complex. The mission of Y-12 includes the manufacture of nuclear weapons components; weapons dismantlement, storage, and evaluation; and, the warehousing of enriched uranium material.

The DOE Office of Inspector General received an allegation that in 2004, non-U.S. citizens were improperly allowed access to a Y-12 leased facility. The objective of this inspection was to evaluate the factual basis of the allegation and, if confirmed, to determine whether control procedures at Y-12 should have prevented such access.

OBSERVATIONS AND CONCLUSIONS

We concluded that the access control procedures at the time of our inspection did not prevent access to Y-12 facilities by illegal aliens. Specifically, we found that:

- Foreign construction workers, using false documents, gained access to the Y-12 site on multiple occasions.

Details of Findings

ACCESS TO Y-12 BY NON-U.S. CITIZENS

We found that foreign construction workers, using false documents, gained access to the Y-12 site on multiple occasions. Specifically, we determined 16 foreign construction workers were illegal aliens. Some of these workers acquired facility access badges and were permitted access to the main Y-12 site, and others were permitted access to an adjacent Y-12 leased facility. Certain information associated with the construction of the Y-12 leased facility, which was planned to store documents up to the Secret-Restricted Data level, was considered Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO). Consequently, these individuals may have had opportunities to inappropriately access this type of information.

Access Control Procedures

We determined that control procedures at Y-12 facilities, which should have prevented unauthorized access, were not implemented. For example, a requirement for all employees working at the Y-12 leased facility construction site to be U.S. citizens was included in the construction solicitation offer and pre-construction briefs; however, this requirement was erroneously not included in the signed contract. While the deletion of the applicable contract clause was a problem, we were also concerned about the apparent reliance on the subcontractor to self-certify the citizenship status of their employees. Also, we learned that the Office of Counterintelligence was not aware of the presence of foreign construction workers at the Y-12 leased facility until notified by the Office of Inspector General (OIG) during this inspection. Counterintelligence checks had not been performed for these individuals to that point.

Use of Fraudulent Documents

We coordinated with the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement (ICE) on the possible use of fraudulent identification by foreign construction workers to gain access to the Y-12 facilities. ICE officials determined that "green cards" used by 16 foreign construction workers were fraudulent. Legitimate "green cards" are used to prove that a foreign national has a legal right to live and work in the United States. Because the "green cards" were fraudulent, the 16 foreign construction workers were considered to be illegal aliens.

Revision of Y-12 Access Policy

We informed the Y-12 Site Office Acting Assistant Manager for Safeguards and Security of these incidents. Following this notification, operations at the Y-12 leased facility were temporarily shut down and additional measures were implemented by Y-12 officials to improve security and control access at the facility. In

February 2005, prior to completion of our inspection, Y-12 officials issued a revised access policy entitled "Citizenship Verification Requirements for Access to the Y-12 National Security Complex." The revised policy addressed the concerns we had raised to Y-12 officials during our review. We plan to include a review of the effectiveness of the revised access policy in future work at Y-12 facilities.

OA Access Control Review

We found that, in January 2004, the DOE Office of Independent and Oversight Performance Assurance (OA) conducted a review of safeguards and security at the Y-12 site, including a review of access control procedures. However, we determined that the OA review did not address the specific access control issues identified in this report.

LESSONS LEARNED

The lessons learned during this inspection have possible broader implications for security at other DOE sites. Therefore, in a separate memorandum to the Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration, we are recommending that they determine what Department-wide actions are warranted.

RECOMMENDATIONS

We recommend that the Manager, Y-12 Site Office:

1. Ensure that the revised access policy is fully and consistently implemented to prevent inappropriate access to Y-12 facilities.

We recommend that the Director, Office of Independent Oversight and Performance Assurance:

2. Review the information provided in this report, and take action to ensure that future OA security reviews at Y-12 and other Department facilities include inspection steps specific to the issues discussed in this report.

MANAGEMENT COMMENTS

Management concurred and provided comments on a draft of this report. NNSA stated that it would make all of its Site Office Managers aware of the findings at Y-12 to ensure that they take similar steps, if necessary, to improve access controls to sensitive DOE sites.

The Office of Security and Safety Performance Assurance (SSA) explained that access controls have been a recognized weakness across the Government, and that much work is being done to

prevent reoccurrence of the types of issues this report identified. For example, SSA noted that the Department's response to Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," as well as new guidance on prosecution of persons who falsely represent their identities, would strengthen access controls. SSA also stated that the Office of Independent Oversight and Performance Assurance would assess the adequacy and effectiveness of the corrective actions implemented by Y-12 in response to this report.

Management's comments are included in their entirety at Appendix B.

INSPECTOR COMMENTS

Management's comments were responsive to our recommendations. We note that at the time of the incidents identified in our report, NNSA had policies in place to control access at Y-12 and other NNSA sites. These policies failed to prevent the deficiencies we identified at Y-12. In that regard, the effective implementation of not only the corrective actions at Y-12, but the implementation of Presidential Directive 12 throughout the DOE complex, takes on greater importance.

NNSA pointed out there was no evidence that foreign nationals with fraudulent green cards had access to any UCNI or OUO documents. During our physical inspection of the Y-12 leased facility, we observed UCNI and OUO documents lying unprotected in a construction trailer, which was accessed by the foreign construction workers who are the subject of this report. Thus, these individuals were afforded opportunities to access UCNI, as well as OUO information. We concluded that this situation represented a potentially serious access control and security problem.

Appendix A

SCOPE AND METHODOLOGY

We identified and reviewed applicable DOE regulations and other key documents applicable to the inspection. We interviewed Federal and contractor staff assigned to Department field locations in Oak Ridge, Tennessee. We worked with the OIG Office of Investigations and the U.S. Department of Homeland Security's Bureau of Immigration and Customs Enforcement.

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency. Pursuant to the Government Performance and Results Act of 1993 we reviewed performance measures related to security and access control.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

JUN 0 8 2005

MEMORANDUM FOR Alfred K. Walter
Assistant Inspector General
for Inspections and Special Inquiries

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Draft Inspection Report on Y-12's Security Access Controls, 2005-14125

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's draft Inspection Report: "Security Access Controls at the Y-12 National Security Complex." We understand that the IG conducted this inspection based on an allegation that undocumented workers were allowed access to a leased facility at Y-12.

NNSA permits subcontractors to use workers who are not U.S. citizens on projects in unclassified areas of the complex. In accordance with U.S. law, these workers are expected to have proper documentation (permanent resident card, also known as a green card). The subcontractor has the responsibility to determine that its employees are either U.S. citizens or possess valid permanent resident cards. In the cases cited in this report, some of the workers involved possessed fraudulent green cards.

The foreign nationals who possessed fraudulent green cards were in a building that contained business sensitive/non-classified (Unclassified Nuclear Information and Official Use Only) documents. There is no evidence that they had access to any of the documents. No classified information was stored in the building. Classified information is strictly controlled, and uncleared workers with or without green cards, fraudulent or otherwise, would have no access to that information.

The policy for granting access to the Y-12 National Security Complex is currently supported by Standing Order Number SO-Y-12-05-06 (Incorporated into BWXT Y-12 Policy Y-12-006 to be published during August), which became effective February 15, 2005. The order applies to any Y-12 organization requesting a Bear Creek Road (main entrance road into plant) Pass, an uncleared visitor's badge, or uncleared photo badge(s) and, the order applies to **ALL** individuals requiring or requesting access to the Y-12 complex. For the public (employees, visitors, subcontractor employees), verification of legal status must be established by the Visitor Control element before gaining access to the site.

Printed with soy ink on recycled paper

Access is withheld until acceptable proof of legal status (such as Birth Certificates, Certificates of Naturalization, Passports, etc.) can be provided. It is incumbent upon employees hosting visitors, subcontract technical representatives, and/or organizations requesting access to the complex to ensure these visitors are aware of the documentation requirements.

NNSA will make all Site Office Managers aware of the IG's findings at Y-12 to ensure that they take similar steps, if necessary, to improve controls on access by uncleared foreign nationals.

Should you have any questions related to this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: William Brumley, Manager, Y-12 Site Office
William Desmond, Associate Administrator for Defense Nuclear Security
Robert Braden, Senior Procurement Executive
Karen Boardman, Director, Service Center

Department of Energy
Washington, DC 20585

May 25, 2005

MEMORANDUM FOR ALFRED K. WALTER
ASSISTANT INSPECTOR GENERAL
FOR INSPECTIONS AND SPECIAL INQUIRIES

FROM: GLENN S. PODONSKY
DIRECTOR
OFFICE OF SECURITY AND SAFETY
PERFORMANCE ASSURANCE

SUBJECT: Response to the Draft Report on Security Access Controls at the Y-12 National Security Complex – SO4IS015

The Office of Security and Safety Performance Assurance (SSA) has reviewed your May 20, 2005, draft report, "Security Access Controls at the Y-12 National Security Complex." We concur with recommendation 2 in the report, which states that future OA security inspections of Y-12 and other Department facilities include reviews of access control procedures. The Office of Independent Oversight and Performance Assurance (OA), within SSA, reviews the adequacy of access controls on an ongoing basis as part of its inspection program. OA has modified its lines of inquiry to more directly assess the particular issues identified at Y-12 in your report.

Currently, OA is inspecting the Y-12 National Security Complex. As part of the Y-12 inspection, OA will assess the adequacy and effectiveness of the access control measures implemented by Y-12 in response to your audit. The Y-12 final inspection report will be issued in July 2005, which will contain the results of our assessment.

We suggest that the report explain that access controls have been a recognized weakness across the government and that much work is being done to improve access controls and prevent reoccurrence of the deficiencies identified in your report. For example, as part of implementing Homeland Security Presidential Directive (HSPD) – 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, the Department, as well as other government agencies, are putting in place standards, by October 2005 that will be strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation. HSPD-12 will require several forms of identification to prove citizenship and identity and a National Agency Check prior to issuance of an access badge with a "smart" electronic chip. It is our understanding that the Department of Energy (DOE) Inspector General will accredit the identity proofing and the Departmental registration process. In addition, the Office of

Printed with soy ink on recycled paper

Security within SSA is incorporating requirements in its current revision of the DOE physical protection manual that will allow prosecution of individuals who falsely represent themselves as a U.S. citizen or use false documents. Prosecution for these offenses is allowed under existing laws and will be used as a form of deterrence.

If you have any questions, please contact me at (301) 903-3777 or your staff may contact Arnold Guevara, OA's Director of Safeguards and Security Evaluations, at (301) 903-5895.

cc:
M. Kilpatrick, OA-1
M. Combs, SO-1
L. Gasperow, SP-1.2
J. Hawthorne, SO-10
L. Wilcher, SO-20
A. Guevara, OA-10

IG Report No. DOE/IG-0691

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

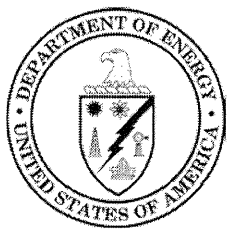
This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

15



U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Protective Force Training at the Department of Energy's Oak Ridge Reservation

DOE/IG-0694

June 2005

Department of Energy

Washington, DC 20585

June 24, 2005

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Protective Force Training at the Department of Energy's Oak Ridge Reservation"

BACKGROUND

The Office of Inspector General received an allegation that a security police officer at the Oak Ridge Reservation was given credit for training that was not received. Wackenhut Services, Inc., the security contractor at Oak Ridge, provides protective force services, including refresher training, for the Reservation. The purpose of our inspection was to determine if the allegation was valid and if, as a consequence, there was any impact on the overall implementation of protective force training at the Reservation.

RESULTS OF INSPECTION

Our inspection confirmed the essence of the facts presented in the allegation. Of greater importance, we concluded that there were material shortcomings in the implementation of the protective force training program at the Oak Ridge Reservation. Specifically, we found:

- Protective force personnel spent, on average, about 40 percent less time on combat readiness refresher training than that specified in the approved Fiscal Year 2004 training plan;

- For some personnel, planned training time was formally reported to the Department as actual training time, resulting in an overstatement of training received;

- Protective force personnel at the Y-12 National Security Complex routinely worked in excess of 60 hours per week, despite a 60 hour maximum threshold for safe operations established in the Department of Energy Protective Force Program Manual. There was evidence that working excessive overtime negatively impacted the ability or willingness of some protective force personnel to complete required physical fitness training; and,

- Some protective force personnel signed attendance rosters for on-the-job refresher training without receiving the training.

The report includes recommendations for corrective actions to address these issues.

Printed with soy ink on recycled paper

MANAGEMENT REACTION

While formally concurring with the findings and recommendations in this report, management articulated areas of disagreement on selected core issues. A summary of our analysis of management's position follows.

During our review, we recognized and acknowledged that planned training time by subject area is only one criterion in evaluating the implementation of a protective force training program; ultimately, the objective is site security and the proficiency of the protective force. However, our review confirmed that Department security experts, based on years of experience, developed the published training standards as Department-wide benchmarks. We concluded that either these standards are valid, and, thus, should be adhered to throughout the complex, or Department security policy should be revised to treat the standards as merely "goals" rather than requirements. And, if so, the Department needs to determine what deviation from the "goals" is acceptable given the security implications at sensitive sites such as Oak Ridge.

Secondly, despite the implication of the comments from management, we did not assess nor did we comment on the overall effectiveness of the training program or the security posture at the Reservation. However, we did note that a Fiscal Year 2004 review at Oak Ridge by the Department's Office of Independent Oversight and Performance Assurance identified several instances where certain tactical skills of some protective force personnel were deficient and recommended improvements to the tactical training being provided.

Management, according to its comments, thought that our concern as to excessive overtime for the protective force was overstated. In support of its position, management cited: the terms of the collective bargaining agreement between Wackenhut and its protective force employees, which management claimed allows protective force personnel to volunteer to work for up to 76 hours per week; the existence of a "post 9-11" variance from overtime limitations cited in the Department's Protective Force Program Manual; and the results of recent protective force physical fitness tests. With regard to the first point, while the collective bargaining agreement is an important issue, we concluded that it may be incompatible with the Department's Protective Force Program Manual's 60 hour threshold, which was designed to ensure that protective force personnel worked at peak physical and mental effectiveness. Further, the variance granted post 9-11 by Department security managers at Oak Ridge was intended only until such time as a sufficient number of protective force personnel could be hired and trained, reducing the need for significant amounts of overtime. Finally, with regard to the protective force fitness tests, the evidence available is apparently mixed. As the report states, we were informed that there has actually been a degradation in the aerobic capacity of the protective force, which is a widely accepted indicator of fitness level.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science and Environment
Administrator, National Nuclear Security Administration
Chief of Staff
Manager, Oak Ridge Office
Manager, Y-12 Site Office
Director, Office of Security and Safety Performance Assurance
Director, Policy and Internal Controls Management
Director, Office of Program Liaison and Financial Analysis

PROTECTIVE FORCE TRAINING AT THE DEPARMENT OF ENERGY'S OAK RIDGE RESERVATION

TABLE OF CONTENTS

OVERVIEW

Introduction and Objective 1

Observations and Conclusions 1

DETAILS OF FINDINGS

Combat Readiness Training 3

Protective Force Overtime 6

On-the-Job Training 7

RECOMMENDATIONS 8

MANAGEMENT COMMENTS 9

INSPECTOR COMMENTS 10

APPENDICES

A. Scope and Methodology 12

B. Prior OIG Reports 13

C. Management Comments 14

Overview

INTRODUCTION AND OBJECTIVE

The Department of Energy (DOE) mission at the Oak Ridge Reservation, which includes the Y-12 National Security Complex (Y-12), the Oak Ridge National Laboratory, East Tennessee Technology Park (ETTP), and the DOE Federal office complex, requires a paramilitary protective force comprised of several hundred security police officers to safeguard the production and storage of nuclear weapons components, special nuclear material, and other sensitive work. The force also includes a Special Response Team (SRT) at Y-12 comprised of specially trained officers who are responsible for engaging and defeating adversaries with advanced capabilities. The protective force is required to complete refresher training each year to ensure that each officer maintains the skills necessary to protect DOE assets from theft and other acts that may cause adverse impacts on national security or the health and safety of the public.

Wackenhut Services, Inc. (Wackenhut), which is a security contractor, provides protective force services, including refresher training, for the Oak Ridge Reservation.

The Office of Inspector General (OIG) received an allegation that a security police officer at the Oak Ridge Reservation was given credit for training that was not received. Therefore, the objective of this inspection was to determine if the protective force training program at the Oak Ridge Reservation was being appropriately implemented.

OBSERVATIONS AND CONCLUSIONS

Our inspection confirmed the essence of the facts presented in the allegation. Of greater importance, we concluded that the protective force training program at the Oak Ridge Reservation was not being appropriately implemented. Specifically, we found that:

- Protective force personnel, on average, spent about 40 percent less time on combat readiness refresher training than that specified in the approved Fiscal Year (FY) 2004 training plan. Further, there is evidence that for some personnel, Wackenhut reported planned rather than actual training time in its quarterly protective force strength and overtime reports to the Department.

- Protective force personnel at Y-12 routinely worked in excess of 60 hours per week. This was in direct contradiction to the DOE Protective Force Program Manual, which established a 60 hour maximum threshold for safe operations. There was

evidence that working excessive overtime negatively impacted the ability or willingness of some protective force personnel to complete required physical fitness training.

- Some protective force personnel signed attendance rosters for on-the-job refresher training without receiving the training.

Wackenhut officials took the position during our review that attempting to correlate specific training tasks to time requirements may not be a valid test of the quality of the protective force training program. They also took the position that there are other performance metrics which are more important, such as meeting the DOE minimum qualification requirements. We recognized this concern as our work evolved in this area. However, we concluded that the Department's safeguards and security specialists established time-related benchmarks for training based on substantial subject matter expertise and many years of training experience. Thus, while our report includes a recommendation that the Department review its protective force training standards, in the absence of new training metrics, we concluded that our evaluation of the training program at the Oak Ridge Reservation relied on the best information available.

The OIG has issued a number of reports concerning protective force training. A listing is provided at Appendix B of this report.

Details of Findings

COMBAT READINESS TRAINING

We found that protective force personnel, on average, spent about 40 percent less time on combat readiness refresher training than that specified in the approved FY 2004 training plan. The training plan was required by DOE Manual 473.2-2, *Protective Force Program Manual*. Further, there is evidence that for some protective force personnel, Wackenhut reported planned rather than actual training time in its quarterly protective force strength and overtime reports to the Department.

Both Title 10 of the Code of Federal Regulations, Part 1046 (10 CFR 1046), *Physical Protection of Security Interests*, and the DOE Protective Force Program Manual require security police officers to complete annual security refresher training to maintain the competencies needed to fulfill their protective force mission. The refresher training is based on lesson plans and associated training hours developed and approved by the DOE National Training Center (NTC). NTC develops protective force training courses, such as firearms training, and assigns a number of hours to each course for the training. Each year DOE sites develop and approve protective force training plans that include training courses developed by the NTC, as well as additional training to address training needs that are specific to the site. For example, the Oak Ridge site-specific training plans for FY 2004 consisted of training courses to provide SRT officers a total of 154 hours of combat readiness refresher training, which included training hours developed by the NTC. The Oak Ridge training plans also provided for non-SRT officers to receive a total of 66 hours of combat readiness refresher training. We were informed by a Wackenhut training official that the majority of protective force training for the Oak Ridge Reservation is based on training courses developed by the NTC. The training plans and associated training hours were approved by Oak Ridge Office management in September 2003 and Y-12 Site Office management in October 2003.

SRT Officers

Training transcripts list all of the training courses taken by a protective force officer and the time designated for each course. Protective force officers attend combat readiness refresher training based on shift assignments; and, travel together as a shift to and from the training center. We reviewed training transcripts, training attendance rosters, payroll charges, and site access records for ten percent of the SRT officers. Our review included SRT officers from four different shifts at Y-12 so as to be representative of the population.

We determined that the SRT officers in our sample spent significantly less time in training than was designated by the approved training plan. Specifically, the SRT officers spent an average of 89 hours on training in various combat readiness skills, but were credited with completing the entire 154 hours of training designated in the approved FY 2004 training plan. For example:

- A training transcript listed seven separate training courses taken on the same day, including a team tactical exercise and chemical and biological warfare training. The approved training plan designated 13.5 hours for this training. However, the SRT officers spent less than 4 hours in training.

- A training transcript gave credit to SRT officers for 12 weapons and team tactical training courses on the same day. The approved training plan designated 16.5 hours for this training. However, the SRT officers spent about 5 hours in training.

- A training transcript gave credit to SRT officers for 12 training courses, on the same day, involving training on vehicle assault, handgun malfunctions, and the use of force. The approved training plan designated 24 hours for this training. However, the SRT officers spent 4.5 hours in training.

Non-SRT Officers

We also determined that non-SRT protective force officers did not spend the amount of time in combat readiness refresher training designated by the approved training plan. The FY 2004 approved training plan designated 66 hours of refresher training for these officers in various combat readiness skills. Based on a limited sample, we found that these officers only received an average of 44 hours of training. However, unlike the SRT officers, who received credit on their training transcripts for the total time designated in the training plan, the non-SRT officers generally only received credit for the hours of refresher training they actually performed.

We compared refresher training at the Oak Ridge Reservation with that provided by a contractor at another major Department site. In contrast, we found the protective force officers at the other site, both SRT and non-SRT officers, on average, spent close to 100 percent of the time designated by their approved training plan in combat readiness refresher training. We also found that the training plans for both sites called for a similar number of hours for combat readiness refresher training.

Reporting

As part of the award fee self-evaluation process, Wackenhut reported that it had met all the training objectives outlined in the Y-12 annual training plan. In addition, quarterly reports submitted to DOE by Wackenhut reflected that SRT officers received the total number of training hours designated in the training plan, not the number of hours they actually trained. We noted the DOE contract allows Wackenhut to group training hours with hours incurred to perform other aspects of the contract. In our view, grouping the reduced training hours with other hours, in conjunction with the Wackenhut reports to DOE of higher training hours, may obscure DOE's ability to evaluate the efficiency of the other operations.

When asked, Wackenhut officials stated that they train to meet DOE standards and not to a specified amount of time. Wackenhut officials view the time designated in the approved training plan as a goal, rather than a requirement. In addition, they indicated that as long as the protective force officers passed the DOE minimum qualification tests, then all the training requirements had been met.

As noted in the Observations and Conclusions section of this report, hours of training may not be the only metric pertinent to evaluation of protective force training. However, according to DOE training officials, significant deviations from the time specified in an approved plan should be reported to the DOE site officials who approved the training plan, as certain combat readiness skills may be diminished if protective force training is significantly reduced. For example, the more time spent in training, the greater the opportunity for protective force personnel to gain increased familiarity with weapons and equipment and to improve their reaction times in emergency situations. Despite a 40 percent reduction in training time, Wackenhut did not notify DOE of the reduced training hours. We believe that the Department should clearly establish whether hours in site annual training plans designated for refresher training are requirements or goals. If it is determined that the training plans are only goals, the Department should determine the extent to which deviations from the training hours in the approved plans are acceptable.

We also noted that the DOE Office of Independent Oversight and Performance Assurance (OA), which is part of the DOE Office of Security and Safety Performance Assurance, identified several instances during a review of selected Oak Ridge Reservation protective force personnel in FY 2004 where certain tactical skills were deficient. In their classified report, OA officials

recommended improvements to the tactical training provided by Wackenhut. We observed that many of the courses that officers completed in fewer training hours than designated in the approved FY 2004 training plan involved tactical training.

PROTECTIVE FORCE OVERTIME

Protective force personnel at Y-12 routinely worked in excess of 60 hours per week. This was in direct contradiction to the DOE Protective Force Program Manual, which established a 60 hour maximum threshold for safe operations. There was evidence that working excessive overtime negatively impacted the ability or willingness of some officers to complete required physical fitness training.

The DOE Protective Force Program Manual states that protective force work schedules should be no more than 60 hours per week and must provide adequate training time and sufficient time off to ensure personnel work at peak physical and mental effectiveness. However, in May 2002, DOE approved a variance for the Oak Ridge Reservation from this requirement to address additional protection needs arising from September 11, 2001 (9-11), with the agreement that additional protective force personnel would be hired to address the increase in overtime and that officers would not work more than 72 hours in any work week. Almost three years after approving the variance, the protective force personnel assigned to Y-12 continue to work excessive amounts of overtime. For example, at Y-12, we found that in FY 2004, 39 percent of SRT officers and 28 percent of other protective force officers worked, on average, more than the 60 hours per week limit in the DOE Protective Force Program Manual. Of these officers, over 40 percent worked more than 70 hours per week, with some exceeding the 72 hour maximum work week established by the variance.

Physical Fitness Training

Some protective force personnel cited excessive overtime as a reason for not completing required physical fitness training. In 10 CFR 1046, it requires that protective force personnel participate in continuing physical fitness training to ensure that they can effectively perform their normal and emergency duties. Until November 2001, an on-site, supervised physical fitness program was in place to meet this requirement. A primary goal of this program was to improve safety by reducing the risk of injury to the protective force. Under the current physical fitness training program, the protective force is paid to train outside of work on an honor system.

We questioned 10 randomly selected protective force officers at Y-12 about their physical fitness training. All of these officers disclosed that they did not always complete the required physical fitness training. They attributed this to the extensive amount of overtime they worked. Several officers reported to us that because they were not able to keep up with physical training, they were concerned about their declining physical fitness. Their concerns appear to be supported by an internal analysis of protective force physical fitness. This analysis showed the aerobic capacity of the protective force, which is a widely accepted indicator of fitness level, had declined by 3.3 percent between 2000 and 2003. We provided information regarding the issue of protective force officers accepting physical fitness training pay, but not completing physical fitness training, to the OIG Office of Investigations.

Overtime Requirements

The National Nuclear Security Administration's (NNSA) Y-12 Site Office Manager cited increased threat levels in the post 9-11 environment, including several major revisions of the Department's Design Basis Threat Policy and other increased security requirements, as factors leading to excessive overtime. The Site Manager indicated that Y-12 would like to do more to address the overtime situation, and, in some cases, has made progress in reducing protective force overtime. However, the Site Manager noted that significant funding constraints combined with increasing requirements have resulted in a continuing problem at Y-12 and other Department sites with protective force overtime. A Wackenhut official indicated that it could take several years before the protective force could be increased in strength enough that overtime requirements would not impact training time. We recognize that addressing current requirements and constraints with existing resources is a complex issue. However, the Department must take steps to realistically address the impact of continued excessive overtime on protective force readiness.

ON-THE-JOB TRAINING

We found that some protective force personnel signed attendance rosters for on-the-job refresher training without receiving the training. On-the-job refresher training for protective force officers is conducted during an officer's normal work activities and includes training in a wide variety of topics, such as conducting security patrols, security alarm assessments, and hasty overt entries. We were told by some protective force officers that, on occasion, they would be asked if they needed training on a topic. If the officers indicated that they did not need training, they were allowed to sign the training attendance roster without receiving any training or demonstrating their proficiency in the training topic.

The rosters were then used to give the officers credit for receiving training. In addition, we identified four instances when a signature on a training attendance roster was falsified, but we were unable to identify who falsified the signatures. The matter regarding the falsification of signatures was referred to the OIG Office of Investigations.

RECOMMENDATIONS

Given the importance of the Oak Ridge Reservation to the Nation's security, we believe actions should be taken to ensure the protective force is properly trained. Therefore, we recommend that the Manager, Oak Ridge Office, and the Manager, Y-12 Site Office, for their respective contracts with Wackenhut Services, Inc.:

1. Determine if the protective force is receiving the appropriate level of training necessary to meet the DOE training requirements for protective force officers.

2. Ensure that Wackenhut reports the actual hours spent in training by protective force personnel rather than the planned hours.

3. Evaluate whether the variance that allowed Oak Ridge to deviate from the DOE Protective Force Program Manual overtime guidelines remains appropriate for the Oak Ridge Reservation protective force.

4. If it is determined that the variance should remain in effect, establish a time period for reevaluating the variance and penalties for exceeding the approved variance.

5. Evaluate whether a supervised physical fitness training program for protective force personnel should be reestablished on-site to improve security readiness and to reduce the safety and health risks to protective force personnel.

6. Strengthen internal controls for the on-the-job training program to ensure that training credit is given only when training has been received.

7. Evaluate the impact of the issues discussed in this report on Wackenhut's award fee.

We also recommend that the Director, Office of Security and Safety Performance Assurance:

8. Review the issues identified in this report and incorporate steps in future assessments at Oak Ridge and other DOE sites to ensure that protective force refresher training is being appropriately implemented.

9. Examine whether hours in site annual training plans designated for refresher training are requirements or goals and develop guidelines regarding the extent, if any, that deviations from the training hours in the approved plans, such as training only to qualify at minimum standards, are acceptable.

MANAGEMENT COMMENTS

Management concurred with the findings and recommendations. Recommendation 2 was revised after comments were received from the Oak Ridge Office. The Oak Ridge Office subsequently advised us that they concurred with the revised recommendation.

Management commented that protective force training is geared toward attaining and demonstrating a desired level of proficiency, rather than mandating a minimum amount of hours to train for the tasks, especially when proficiency has been proven in less than the allotted time. They advised that this "training to standard" is an accepted practice operationally and with the Department's National Training Center. They also advised that evaluations of training by the Government Accountability Office, OA, OIG, and others have found the quality of protective force training meets Departmental requirements.

Management commented that the number of hours worked by the protective force was within the collective bargaining agreement between Wackenhut and the protective force union, and the Department did not need to grant a variance to Wackenhut from meeting the DOE Protective Force Program Manual requirement regarding overtime.

Finally, management commented that the current pass rate for the annual physical fitness tests is approximately 98 percent, which lends credence to the success of the offsite training program.

Management's comments are included in their entirety as Appendix C to this report.

INSPECTOR COMMENTS

Management's comments indicated a fundamental disagreement on the core issues in our report. We carefully considered the positions asserted by management and did not find them compelling.

We recognize and acknowledge that planned training time by subject area is only one criterion in evaluating the implementation of a protective force training program. However, our review confirmed that Department security experts, based on years of experience and much consideration, developed the published training standards as a Department-wide benchmark. We concluded that these standards either are valid, and thus should be adhered to throughout the complex, or that Department security officials should declare the standards to merely be goals rather than requirements. If the standards are merely goals, the Department needs to determine what variation from the goal is acceptable given the security implications at sensitive sites such as Oak Ridge.

Also, we did not assess the overall effectiveness of the training program at Oak Ridge, nor did we evaluate the security posture at the Reservation. However, we did note an FY 2004 review at Oak Ridge by the Department's Office of Independent Oversight and Performance Assurance identified several instances where certain tactical skills of some protective force personnel were deficient, and recommended improvements to the tactical training being provided.

Management disagreed with our concern regarding excessive overtime for the protective force. In support of its position, management cited the terms of the collective bargaining agreement with Wackenhut, which management claims allows protective force personnel to volunteer to work for up to 76 hours per week; the existence of a "post 9-11" variance from overtime limitations cited in DOE's Protective Force Program Manual; and, the results of recent protective force physical fitness tests.

With regard to the first point, while the collective bargaining agreement is an important issue, we concluded that it was incompatible with the stated objective of the DOE Protective Force Program Manual to ensure that protective force personnel worked at peak physical and mental effectiveness. Further, the variance granted post 9-11 by the Department security managers at Oak Ridge was intended only until such time as a sufficient number of protective force personnel could be hired and trained. Finally, with regard to the protective force fitness tests, as the report states, we

were informed that there has actually been a degradation in the aerobic capacity of the protective force, which is a widely accepted indicator of fitness level.

Appendix A

SCOPE AND METHODOLOGY

The fieldwork for this inspection was conducted between November 2004 and March 2005. The inspection included a comparison of training, payroll, and site access records for FY 2004 for 21 protective force officers that were randomly selected to represent all the sites and varying shifts. The inspection also included:

- Interviewing 45 people who administer, deliver or receive protective force training;
- Reviewing FY 2004 annual training plans approved by the Y-12 Site Office and the Oak Ridge Office;
- Reviewing the Y-12 Site Office and Oak Ridge Office contracts for protective force services; and,
- Interviewing Federal and contractor security personnel.

We found that the protective force contracts for the Oak Ridge Reservation contained appropriate performance measures to address protective force training, pursuant to the Government Performance and Results Act of 1993. This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Appendix B

PRIOR OIG REPORTS

The OIG has issued the following reports addressing protective force training:

- *The Department's Basic Protective Force Training Program*, DOE/IG-0641, March 2004.
- *Protective Force Performance Test Improprieties*, DOE/IG-0636, January 2004.
- *Management of the Department's Protective Forces*, DOE/IG-0602, June 2003.
- *The Restructure of Security Services by the Oak Ridge Operations Office*, DOE/IG-0487, October 2000.
- *Security Overtime at the Oak Ridge Operations Office*, ER-B-00-02, June 2000.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MAY 25 2005

MEMORANDUM FOR Alfred K. Walter
Assistant Inspector General
for Inspections and Special Inquiries

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to IG's Draft Report on Protective Force Training

The National Nuclear Security Administration (NNSA) appreciates the opportunity to have reviewed the Inspector General's (IG) draft inspection report: "Protective Force Training at the Department of Energy's Oak Ridge Reservation." We understand that this inspection was based on an allegation that a security police officer at the Oak Ridge Reservation was given credit for training that was not received. After reviewing the report and the comments that have been submitted to us, we do not believe that there is any basis for the allegation. We further believe that the IG did not take into consideration the methodology of training to standards rather than training to compliance nor did they take into consideration the contractual agreement with the appropriate Labor Union. We are, however, forwarding the information about signing attendance rosters without receiving training to the Investigations unit. Below are NNSA's comments to some of the report's conclusions.

- **Signing attendance rosters without receiving training** – We take the IG's comment that some protective force personnel signed attendance rosters for on-the-job training without receiving the actual training quite seriously. In fact, that matter has been referred for Investigation and therefore it is not appropriate to comment on these allegations until such time as the Investigation has been completed.

- **Spending less time on training than specified in the training plan** – The IG is correct when stating that the training syllabus, or plan, and amount of time needed to train to the plan is established by security subject matter experts. The training plan referred to by the IG is developed annually to meet Federal regulations and departmental orders. The individual lesson plans derived from the syllabus are developed by the

Printed with soy ink on recycled paper

National Training Center for the Basic Security Police Officer (SPO) Training Course, the SPO III Basic Qualification Course, and other specialty courses. However, the lesson plans are based on an entry level of competence assumed of individuals. The recommended hours to train are designed to ensure mastery of the knowledge, skills, and abilities necessary to meet task requirements. Actual hours needed to train vary depending on class size, individual levels of competence, combined training, and prior skills and experience of students. The NNSA methodology of operations is based on working efficiently and effectively rather than being strictly compliance driven. Departmental orders recognize this efficiency by acknowledging that if individuals satisfactorily demonstrate a knowledge, skill, or ability they may be exempt from portions of formal annual refresher training. The efficiency in this is that we train to a standard (a term of art) which is an accepted practice operationally and with the Department's National Training Center. Therefore, while the IG may be correct in identifying a 40 percent delta between planned and actual training, there is no indication that the results obtained through training to a standard is any less effective or efficient than to generic training plans. Contractually and administratively the reporting of training accomplished citing planned hours rather than actual hours is a consequence of requirements. The security contractor is reimbursed only for actual hours worked regardless of whether the individual is in a training status or an operational status.

- **Routinely working in excess of 60 hours a week** – The IG is correct in mentioning that the Protective Force Program Manual establishes a 60 hour maximum threshold for safe operations. However, the Manual also states work schedules are to be based on, and be consistent with, collective bargaining agreements and with contractual requirements. In this case the security contractor entered into an agreement with the International Guards Union of America, Local Number 3, that allows up to 62 hours of mandatory work. The agreement also allows Security Police Officers to volunteer for up to a total of 76 hours a week. Since the Manual states that hours worked must be consistent with appropriate collective bargaining agreements, there is no discrepancy to be noted. It is important to note that prudently managed overtime worked is an appropriate management tool, which can result in keeping costs under control with changing threat conditions. With the changes in the Design Basis Threat (DBT) and time required to recruit, train and obtain clearances for new SPOs, overtime is a necessary requirement to accomplish mission needs. The role of Federal oversight is to ensure that the security contractor effectively and efficiently manages the amount of overtime experienced and to continue to institute actions to minimize overtime. This oversight includes actions by the contractor, with Federal involvement, to appropriately move physical fitness training to off-shift time periods, disestablish the Relief Shift and

assign all personnel to rotating shift duties, conduct training on scheduled days off, and to identify and eliminate unnecessary positions.

Regarding the recommendations, we generally agree with all but two of the recommendations but request that the IG review their recommendations in light of our comments, as stated above.

Recommendations

1. **Determine if the protective force is receiving the appropriate level of training necessary to meet the DOE training requirements for protective force officers.**

Management Comment

Concur.

WSI-OR's Annual Refresher Training consists of all tasks and requirements contained in DOE Manual 473.2-2, as well as various job tasks identified in site specific job analyses for each position that tests or trains necessary skills for daily operations, legal authority, and other compliance training. Combat Readiness Training is primarily conducted onsite, on-the-job, during shift drills, during limited scope performance tests, and engagement simulation system exercises. Past and ongoing inspections, reviews, audits, and assessments confirm that the appropriate level of training has been and continues to be given to meet DOE training requirements. This includes formal reviews by the DOE Office of Independent Oversight and Performance Assurance (OA), General Accounting Office audits, Office of Inspector General audits/inspections, YSO assessments, and assessments by the DOE National Training Center.

2. **Ensure that Wackenhut reports the actual hours spent in training by protective force personnel rather than the planned hours.**

Management Comment

Concur

Since we stated that "training to standard" is a current and acceptable practice, we will take the appropriate actions to ensure actual hours for training are reported rather than planned hours.

3. **Evaluate whether the variance that allowed Oak Ridge to deviate from the Protective Force Program Manual overtime guidelines remains appropriate for the Oak Ridge Reservation Protective force.**

Management Comment

Concur

The overtime activity for WSI-OR has been under consistent Federal review since the inception of its contract. Due to the events of 9/11 and changes to the Design Basis Threat, the overtime has been both necessary and justified. Reduction of overtime continues to be a significant goal for WSI-OR. However, the primary means to meet that goal is to increase the staffing level of Q-cleared and Human Reliability Program (HRP) certified SPOs. WSI-OR, in concert with DOE/NNSA/YSO, has been attempting to hire, train, and field additional protective force personnel. However, the Human Reliability Program and security clearance processes have greatly restricted attempts to utilize additional personnel to reduce current overtime requirements. The process for obtaining a Q-clearance currently ranges from 12 to 24 months, unless mitigating circumstances are encountered. Until Q-cleared/HRP-certified staffing levels are increased, overtime will be required to meet requirements. The Site Safeguards and Security Plan (SSSP), which lists all variances to Federal requirements, is reviewed annually. Justification for maintaining the overtime variance was evaluated as part of the latest review of the SSSP. Accordingly, the variance will remain in effect, as well as the overtime agreement dated April 11, 2002, in the IGUA bargaining unit agreement.

4. **If it is determined that the variance should remain in effect, establish a time period for reevaluating the variance and penalties for exceeding the approved variance.**

Management Comment

Concur

As previously stated, the variance will remain in effect. Mission requirements and available resources will be evaluated on an annual basis to determine whether the variance will be eliminated. Notwithstanding, the overtime agreement with the IGUA bargaining unit is the primary authority for SPOs to exceed the overtime limits described in DOE M 473.2-2. If necessary, the award fee process will be the vehicle used to penalize WSI-OR for exceeding the variance limitations. Impacts will be determined on a case-by-case basis.

5. **Evaluate whether a supervised physical fitness training program for protective force personnel should be reestablished onsite to improve security readiness and to reduce safety and health risks to protective force personnel.**

Management Comment

Concur

The current physical fitness training program conducted offsite is in full compliance with 10 CFR 1046 and has been approved by the Federal entity. The training is for the purpose of ensuring that SPOs maintain the requisite physical fitness for effective job performance and to enable the individual SPO to pass the applicable annual physical fitness requalification test without suffering any undue physical injury. The late 2001 decision to allow the program to be conducted on an individual basis offsite was based on the fact that less than 30 percent of the SPOs were actually being relieved from duty to conduct physical training due to mission requirements. Reestablishing the physical fitness training program onsite would require a large number of relief personnel and potentially double the amount of overtime currently required. The current WSI-OR pass rate for annual SPO fitness tests is approximately 98 percent, which lends credence to the success of the offsite training program. The program's success will continually be monitored to determine if a more cost efficient program could reduce greater pass results. Action complete.

6. **Strengthen internal controls for the on-the-job training program to ensure that training credit is given only when training has been received.**

Management Comment

Concur

The OIG basis for this recommendation is that "some protective officers" were asked on occasion if they needed training on a topic. The OIG report states that the officers informed them that they would be allowed to sign training attendance rosters without receiving any training or demonstrating their proficiency in the training topic. Without specific details, it is difficult to determine whether a training violation actually occurred. It is possible that the officers were referring to any number of tasks for which formal training is not required. An example of this is "Groom and Prepare for Duty," an on-the-job training (OJT) task listed in the 2004 ATP. If a supervisor can visibly determine that a SPO has clearly demonstrated

his/her knowledge of the standard, there is no need for formal training, yet a record of the training would exist. However, WSI-OR will continue to monitor the OJT Training Program to ensure all training is conducted to standards and that no training credit is granted unless the standards have been meet.

7. **Evaluate the impact of issues discussed in this report on Wackenhut's award fee.**

Management Comment

Concur

The issues described in this report as well as a myriad of additional factors are considered in the award fee process. It has been concluded and validated by the National Training Center that "training to standard" is not only an acceptable practice, but a cost efficient practice. Therefore, issues described in this report, other than those to be reviewed by the Investigative Branch of the OIG, do not appear to be a basis for negatively impacting past or future award fee earned by WSI-OR. Upon completion of the of the IG's investigation of alleged improprieties, consideration will be given to the impact of award fee to be earned by WSI-OR.

Should you have any comments related to this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: William Brumley, Manager, Y-12 Site Office
William Desmond, Associate Administrator for Defense Nuclear Security
Robert Braden, Senior Procurement Executive
Karen Boardman, Director, Service Center

Department of Energy
Washington, DC 20585

May 25, 2005

MEMORANDUM FOR ALFRED K. WALTER
ASSISTANT INSPECTOR GENERAL
FOR INSPECTIONS AND SPECIAL INQUIRIES

FROM: GLENN S. PODONSKY
DIRECTOR
OFFICE OF SECURITY AND SAFETY
PERFORMANCE ASSURANCE

SUBJECT: Response to Draft Inspection Report on Protective Force Training at the Department of Energy's Oak Ridge Reservation – SO5IS003

Attached are comments on your May 2005 draft report, "Protective Force Training at the Department of Energy's Oak Ridge Reservation." These comments are from the Oak Ridge Operations Office (ORO) (see attachment) and the Office of Security and Safety Performance Assurance (SSA), provided below.

Both organizations concur with the recommendations in this report with comment. A common observation from the two organizations is that the report should be revised to clearly identify issues and concerns with the Y-12 National Security Complex (Y-12). The additional clarity will help in addressing the recommendations since the Y-12 associated issues/concerns will involve the National Nuclear Security Administration instead of the ORO, the Office of Science, or the Office of Environmental Management.

As stated in the attached memorandum, ORO concurs with recommendations 1 through 7 with comment. ORO intends to review the areas pointed out as concerns or issues by your office and determine how training can be improved. However, ORO noted that the audit did not consider the terms and conditions established in the DOE-Wackenhut contract and the employee bargaining union agreement which establish financial and human resource controls to ensure responsible management of security police officers (SPOs) and federal funding. In addition, ORO comments that your audit makes no assessment of the proficiency of the SPOs as a result of the current training program, stating that training is geared toward attaining and demonstrating proficiency versus complying with estimated training hours which your audit raises as a concern.

SSA concurs with recommendations 8 and 9, in the report, which state that SSA review the adequacy of protective force refresher training at the Oak Ridge Reservation and other DOE sites, as well as the acceptability of deviations from the annual training plans for core protective force skills. The Office of Independent Oversight and Performance Assurance (OA), within SSA, reviews the adequacy of protective force training, including refresher training, on an ongoing basis as part of its inspection program.

Printed with soy ink on recycled paper

Currently, OA is inspecting the Y-12 protective force program. As part of the Y-12 inspection scope, OA will assess the adequacy of the training program and the effectiveness of training to prepare the Y-12 protective force to perform its mission. The Y-12 final inspection report will be issued in July 2005.

If you have any questions, please contact me at (301) 903-3777 or your staff can contact Arnold Guevara, Director, Office of Safeguards and Security Evaluations at (301) 903-5895.

Attachment: (As stated)

cc:
G. Boyd, ORO
D. Erbschloe, SC-3
M. Kilpatrick, OA-1
A. Guevara, OA-10
M. Combs, SO-1
J. Hawthorne, SO-10
L. Wilcher, SO-20
L. Gasperow, SP-1.2
D. Thress, ORO/ORNL
J. Penry, ORO/FM-70
J. Miller, ORO/FM-733
M. Lewis, ME-100

Attachment

OAK RIDGE OFFICE
RESPONSE TO OFFICE OF INSPECTOR GENERAL DRAFT INSPECTION REPORT
"PROTECTIVE FORCE TRAINING AT THE DEPARTMENT OF ENERGY'S OAK RIDGE RESERVATION"

GENERAL COMMENTS:

The Oak Ridge Office (ORO) has reviewed the Office of Inspector General (OIG) Draft Report, "*Protective Force Training at the Department of Energy's Oak Ridge Reservation.*" Much of the report identifies issues and concerns specific to the Wackenhut Services Incorporated (WSI) Y-12 protective force. Therefore, comments and recommendations specific to Y-12 will be addressed by the National Nuclear Security Administration. Although we question the OIG conclusion that the protective force training program is not being properly implemented, Oak Ridge Office (ORO) will, subject to some elaboration, concur with the ORO-related recommendations.

First, a significant premise on which the most serious training allegations are based seems inconsistent with the Department of Energy's (DOE) training doctrine and, to some degree, the implications of the 2004 ORO Training Plan. The National Training Center has indicated, for instance, that the expectation (in relevant DOE Orders) is that training's purpose is to facilitate task proficiency, not mandate a minimum amount of hours to train for those tasks, especially when proficiency has been proven in less than the allotted time. Furthermore, portions of the training plan suggest that "training to standard" is the plan's expectation. For instance, the Implementation section asserts, "The ultimate goal of all training at WSI-OR is for the student to *demonstrate proficiency* in performing assigned duty tasks." Moreover, the plan's Approach to Training section proclaims, "WSI-OR training is designed for all learners to *achieve task mastery*, as opposed to a bell curve distribution...." Lastly, evaluations conducted during Site Security Surveys, Office of Independent Oversight evaluations and award performance evaluations, and recently by the General Accountability Office, have found the quality of protective force training to meet Departmental requirements.

Second, since the DOE-Wackenhut contract is a Time and Materials contract, the direct productive labor hours are not identified by individual tasks and, thus, is not a criterion for billing hours. Individuals are paid for actual hours worked, whether in training or in security positions at a site.

Third, WSI-Oak Ridge (OR) has implemented overtime agreements with the bargaining units, in accordance with the provisions of DOE Order 473.2, Protective Force Program and DOE Manual (M) 473.2-2, Protective Force Program Manual. Thus, a "variance" allowing deviation from the Protective Force Program Manual was not needed.

Fourth, the WSI-OR physical fitness program seemingly complies with 10 Code of Federal Regulations 1046, which requires protective force personnel to participate in continuing physical fitness training. It does not, however, dictate a specific number of workout sessions or specify any other requirements of the program. The collective bargaining agreements contemplate

1

paying Security Police Officers (SPO) for off-duty physical training. The current WSI-OR pass rate for annual SPO fitness tests is almost 98 percent.

RESPONSE TO RECOMMENDATIONS:

That the Manager, Oak Ridge Office for the contract with Wackenhut Services Incorporated:

Recommendation 1: Determine if the protective force is receiving the appropriate level of training necessary to meet the DOE training requirements for protective force officers.

Response: Concur, under the assumption that the recommendation seeks a determination about whether training to accomplish "tasks" within the allotted times is more fitting than simply training for a requisite number of hours, even if the respective protective force officer has accomplished the tasks the training has contemplated.

Recommendation 2: If it is determined that the protective force is meeting the DOE training requirements by training in less hours than designated in the approved training plan, reduce the maximum number of billable hours in the Wackenhut contract to reflect the hours that are actually spent in training.

Response: ORO concurs with examining whether the DOE-Wackenhut "Time and Materials contract", under which SPOs are paid for actual hours worked (whether in training or in security positions) might permit a reduction in so-called "billable hours."

Recommendation 3: Evaluate whether the variance that allowed Oak Ridge to deviate from the *Protective Force Program Manual* overtime guidelines remains appropriate for the Oak Ridge Reservation protective force.

Response: ORO concurs. Although no such "variance" is required, ORO will evaluate whether the Wackenhut overtime agreements with bargaining units seem consistent with relevant provisions of DOE Order 473.2, Protective Force Program and DOE M 473.2-2, Protective Force Program Manual.

Recommendation 4: If it is determined that the variance should remain in effect, establish a time period for reevaluating the variance and penalties for exceeding the approved variance.

Response: ORO concurs. Although no such "variance" is required, ORO will evaluate whether the Wackenhut overtime agreements with bargaining units seem consistent with relevant provisions of DOE Order 473.2, Protective Force Program and DOE M 473.2-2, Protective Force Program Manual.

Recommendation 5: Evaluate whether a supervised physical fitness training program for protective force personnel should be reestablished on-site to improve security readiness and to reduce the safety and health risks to protective force personnel.

Response: ORO concurs.

Recommendation 6: **Strengthen internal controls for the on-the-job training program to ensure that training credit is given only when training has been received.**

Response: ORO concurs. We will ensure that WSI-OR monitors the on-the-job training program to ensure all training is conducted to standard and no training credit is granted unless the standards have been met.

Recommendation 7: **Evaluate the impact of the issues discussed in this report on Wackenhut's award fee.**

Response: ORO concurs. ORO will evaluate the impact of the issues discussed in this report during the next performance evaluation period.

IG Report No. DOE/IG-0694

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

16

Levernier, Richard

From: Levernier, Richard
Sent: Wednesday, September 07, 2005 4:06 PM
To: 'tbiggs@osc.gov'; 'cmcmullen@osc.gov'
Cc: 'whistle47@aol.com'
Subject: OSC File No. DI-02-0572

The DOE/National Nuclear Security Administration (NNSA) posted an independent review commonly known as the "Mies Report" of security on its web site on September 1, 2005. I have attached the report for your convenience. This report is very critical of DOE/NNSA security management. This very recent report echoes the findings of the 1999 President's Foreign Intelligence Advisory Board (PFIAB) on DOE titled *Science at its Best / Security at its Worst* and more significantly from my perspective corroborates the issues identified in my Whistleblower Disclosure. The transmittal memorandum of the report (paragraph 5) states, " Of greatest concern, our panel finds that past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges that exist within DOE and NNSA. Many of these issues are not new; many continue to exist because a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA. Accordingly, our panel strongly recommends that NNSA continue to work within DOE to develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations."

The Mies Report specifically corroborates many of the critical issues I identified in my Whistleblower Disclosure almost 4 years ago. These issues include the lack of necessary qualifications of security personnel, a lack of security oversight, a flawed vulnerability assessment and performance test process that distorts the status of security and provides, "a false sense of security"; a general lack of protective force capability resulting in numerous exploitable vulnerabilities for a determined terrorist adversary, i.e., inadequate guidance and training in several significant areas (such as adversary pathways, chemical and biological weapon defenses, and recapture, recovery, and pursuit) and inadequate alarm systems.

It is requested that the Office of Special Counsel evaluate the Mies Report in conjunction with my comments submitted on August 26, 2005 concerning the DOE response to my Whistleblower Disclosure. It is also requested that this message and the entire text of the Mies Report be included in the public record on this matter.

Thank you,

Richard J. Levernier
Senior Technical Advisor
Office of Security, SO-1
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290
Voice (301) 903-2178
Fax (301) 903-2568

2005-05-02_Independent_NNSA_Se...

17

2 May 2005

From: Richard W. Mies, Admiral USN (Retired)

To: NNSA Administrator, Ambassador Linton Brooks

Subject: Independent NNSA Security Review

Enclosure (1) NNSA Security - An Independent Review

1. Background. Since President Franklin Delano Roosevelt created the American nuclear weapons program by informal directive in October 1939, preserving nuclear security has been a national imperative. It also has been an exceptional challenge. Many of the difficulties inherent in nuclear security - creating an open yet secure atmosphere for world-class nuclear weapons science, managing contact with foreign scientist, securing and accounting for minute quantities of special nuclear materials - have been part of the program since its birth. Modem technology keeps bringing new challenges. Cyber security is one example; the proliferation of microelectronic devices – cellular, telephones, personal data assistants, increasingly powerful laptop computers, and high capacity computer memory devices – has created a new array of security challenges.

Federal oversight of the nuclear weapons program has evolved through the years beginning with the Uranium Committee in late 1939; transitioning to the National Defense Research Committee, then the Office of Scientific Research and Development, and then the Manhattan Project during World War II; residing in the newly created Atomic Energy Commission (AEC) in 1947; transferring to the Energy Research and Development Administration in 1975; and finally shifting to the newly created Department of Energy (DOE) in 1977.

In 1999, Congress, reacting in part to security lapses, transferred responsibility to a semiautonomous agency, the National Nuclear Security Administration (NNSA). Section 3212 of NNSA's Title XXXII legislative charter gave the NNSA Administrator authority over, and responsibility for, all programs and activities of NNSA, including safeguards and security (S&S). In practice, although NNSA is closely involved in security policy development, separate DOE offices outside NNSA develop security policy and conduct independent security audits and inspections.

Nuclear security, always important, has become even more critical in the aftermath of September 11. A previous commission highlighted a problem in the entire nuclear weapons complex - the aging federal and contractor scientific and technical workforce - which also pertains to the approximately 150 federal security professionals in NNSA. In

2002, another commission report identified the new challenges facing DOE in operating premier scientific instructions in the 21" century in a manner that fosters scientific excellence and promotes the missions of the Department, while protecting and enhancing national security. Finally, a series of well-publicized security incidents had, by the summer of 2003, led Energy Secretary Spencer Abraham to direct NNSA to aggressively and broadly improve nuclear security.

2. Against this background, NNSA Administrator Linton Brooks established two groups to assess long-range issues affecting security management and protection. The first study group analyzed the federal security workforce; this study, broader in scope, examines a multitude of factors that affect NNSA's security programs. For the past 18 months, we have independently reviewed security at NNSA sites. This report describes our analyses, summarizes our findings, and recommends ways to improve NNSA's security. We interviewed professionals who directly manage and indirectly support the security programs throughout the NNSA complex, including those at Los Alamos, Pantex, Oak Ridge, Livermore, Sandia, Nevada, and Savannah River and DOE and NNSA headquarters. We also reviewed past reports and numerous other documents relating to the nuclear security program and received briefings on topics germane to this study from responsible officials in DOE and NNSA.

We were given a very broad charter to take a strategic look at how security within DOE/NNSA is organized and structured, the interrelationships between various security disciplines, and the existing security policies, procedures, and practices in place to recommend possible improvements. We were specifically not chartered to look at specific security incidents and individual NNSA organizations in isolation.

3. Enclosure (1) forwards the detailed observations and recommendations of our study group. Because of the comprehensive nature and sensitivity of the security issues addressed in our review, enclosure (1) has been classified.

4. Our review consists of 13 sections which address specific areas of security within DOE/NNSA. An unclassified summary of our general observations in each of these areas follows:

Culture: NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission:

- Lack of a team approach to security
- Disparate views and an underappreciation of security across the enterprise, such that security is not fully embraced as integral to mission

- Ingrained organizational relationships that inhibit an enterprise approach to security
- A bias against training
- An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards
- Lack of trust in the security organization
- An absence of accountability.

Roles, Responsibilities, and Relationships: The small size of the NNSA organization greatly impedes its effectiveness with the DOE headquarters bureaucracy. Although NNSA has made good progress by consolidating security functions, responsibility for security as a process is still fragmented and, along with authority and accountability for security, is not adequately embedded in individual and line management responsibilities. Until recently, staffs were organizationally misaligned. Security personnel with sufficient certification, training, rotation, and broad experience are lacking. Security collaboration between DOE/NNSA and DoD and among individual security disciplines within DOE is lacking. NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, divorcing itself from day-to-day oversight.

Security Policy: The NNSA enterprise lacks a comprehensive strategic security plan. Policy collaboration is lacking between DOE and DoD, internally within DOE/NNSA headquarters, between headquarters and the sites, and among sites. NNSA does not have adequate staffing to direct policy to the field or facilitate site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in implementation. No effective system is in place for verifying documented security guidance and direction.

Cyber System Security: DOE/NNSA cyber security policies, procedures, and practices are less mature than their counterparts in other security disciplines. NNSA is resource poor in terms of secure or classified networks and access terminals. Insufficient resources have been devoted to address many of its cyber security issues, particularly the insider threat. Cyber security implementation varies widely throughout NNSA because of the lack of an enterprise approach, inadequate funding, insufficient cyber security personnel and expertise, and inadequate collaboration among DOE and NNSA cyber security organizations. Cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. This stovepipe approach to security has hindered the development of a more comprehensive coordinated approach to securing NNSA information assets.

Counterintelligence: The DOE/NNSA counterintelligence program suffers from a dysfunctional relationship between counterintelligence offices, insufficient collaboration with the other security disciplines, lack of a proactive approach to protection of information, and insufficient emphasis on the insider threat. Counterintelligence budget allocations do not appear to be aligned with program priorities. Finally, performance objectives designed to promote counterintelligence initiatives to deter, prevent, and preempt espionage activities are lacking.

Site Safeguards and Security Plans (SSSP). Vulnerability Assessments NA). and Performance Testing: A number of factors -the shortage of experienced VA analysts, increase in work-load resulting from the new design basis threat (DBT), lack of a comprehensive VA training program, overreliance on a few VA tools, and lack of a rigorous, institutionalized VA approach -detract from the validity and consistency of VAs across the NNSA complex. In addition, weaknesses and wide variations in SSSP limited scope performance testing and force-on-force exercises distort physical security assessments across the complex, promote a false sense of security in selected areas, and complicate prudent allocation of security resources to address potential vulnerabilities.

Protective Force: NNSA lacks a consistent approach for validating protective force manning; because of wide variations in site approaches, determining whether site protective force can adequately meet the requirements of the new DBT remains problematic. Protective force performance is degraded by an excessive backlog in security clearances, inadequate guidance and training in several significant areas (such as adversary pathways, chemical and biological weapon defenses, and recapture, recovery and pursuit), and a lack of collaboration with vulnerability assessment experts, FBI, and local law enforcement officials. Response plans, target folders, and central alarm station systems need upgrading to improve protective force readiness.

Security Incidents and Inquiries: The reporting, investigation, monitoring, and analysis of security incidents within NNSA are hindered by inconsistent practices, redundant reporting, and inadequate reviews. More formal and disciplined processes are needed to ensure the underlying causes of incidents are identified and addressed, appropriate corrective action is effectively implemented, and lessons learned are disseminated within NNSA to mitigate against recurrence.

Design Basis Threat (DBT) Implementation: There has been insufficient collaboration between DOE and DoD and among NNSA sites in translating the intelligence community's postulated threat into security requirements. As a result, NNSA security standards differ:

- from those of DoD nuclear weapons facilities, because DOE/NNSA has taken a different approach to dealing with the postulated threat than that of DoD, and

- from site to site, because sites interpret terms such as insider threat, mission-critical facilities, escorting policies, and improvised nuclear devices differently.

Determining whether NNSA will meet DBT implementation objectives by FY06 is difficult: the process for managing the program and funding requirements largely depend on the sites' interpretations of DBT requirements.

Security Research and Development (R&D) Programs: DOE/NNSA lacks a strategic vision and plan for R&D, procurement, and installation of technologies to improve security across the enterprise. There is no centralized technology component with the department to oversee such a plan. As a consequence, security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without benefit of expert headquarters oversight and complex-wide collaboration. There is no robust technology R&D foundation for an advanced protection strategy.

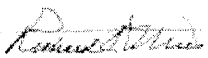
Nuclear Materials and Waste Storage: DOE/NNSA lack an enterprise-wide plan for consolidation of Special Nuclear Material (SNM). A lack of collaboration between NNSA and other elements of DOE, such as EM and NE, may preclude some secure and cost effective alternatives for consolidation from consideration. DOE /NNSA should seek to make greater use of underground storage. Some radiological waste storage areas may lack adequate protection against sabotage which could cause wide-area radiological dispersal.

Security Resources and Requirements: NNSA has made good progress in implementing a planning, programming, budgeting and evaluation (PPBE) process, but much remains to be done. The lack of an enterprise approach to security planning, inconsistent site-to-site interpretation and implementation of security resource requirements, lack of collaboration among the participants in the budget process, lack of a centralized budget validation process, and a cumbersome and unresponsive reprogramming process complicate rational resource planning, programming, budgeting, and evaluation to meet evolving security needs.

Security Contracting: The contractual relationships for security which NNSA has inherited are varied and adverse. Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting-with appropriate focus on security as a key element of maintenance and operations (M&O) contractor performance-is a very positive, overdue step. NNSA has been operating under the Department of Energy Acquisition Regulation (DEAR); however, NNSA requires a unique set of tailored acquisition regulations and a common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

5. Our panel has provided a number of detailed recommendations to address each of our specific concerns outlined in general terms above. Of greatest concern, our panel finds that past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges that exist within DOE and NNSA. Many of these issues are not new; many continue to exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA. Accordingly, our panel strongly recommends that NNSA continue to work within DOE to develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations.

6. Additionally, our panel fully supports the findings and recommendations of the Chiles panel on the need for improved career development, assignment rotation, training, professional qualification, and certification of NNSA security personnel. All security systems ultimately depend on trust. Committed, well trained, and experienced people can overcome organizational deficiencies; but no organizational improvements can overcome uncommitted, poorly trained, or inexperienced people.



Richard W. Mies
Admiral, US Navy (Retired)

NNSA SECURITY

An Independent Review

April 2005

CONTRACT NUMBER DEAM5204NA99608

SAGE
Systems Technologies, LLC
An Alaska Native Corporation (ANC)

LMI
GOVERNMENT CONSULTING

Acknowledgments

This study was conducted under the leadership of ADM Richard W. Mies USN (Retired). Sage Systems Technologies, LLC, and LMI supported the effort. The primary contributors to this report include the following:

- ADM Richard W. Mies USN (Retired), Study Director
- Mr. Paul Grimm
- Mr. Gregory R. English
- Mr. Victor A. Lambson
- Mr. Fremont G. Mortensen
- Mr. Scott W. Patrick
- Mr. Matthew R. Pincock
- Mr. John F. Seward

The study team is grateful for the support of numerous individuals at both NNSA and DOE, who provided the information that allowed us to develop our findings and recommendations. Other contributors to the effort include Mr. Bill Coleman, Mr. David Dietz, and Mr. Ronnie Edge.

Contents

Acknowledgments vii

Section 1 Introduction 1-1

1.1 Background 1-1

1.2 Approach 1-2

1.3 Report Organization 1-3

Section 2 Culture 2-1

2.1 Background 2-1

2.2 Summary 2-1

2.3 OBSERVATIONS 2-2

2.3.1 Lack of Team Approach 2-2

2.3.2 Cultural Opposition 2-2

2.3.3 Bias against Training 2-3

2.3.4 Lack of Trust 2-4

2.3.5 Absence of Accountability 2-4

2.4 Recommendations 2-5

Section 3 Roles, Responsibilities, and Relationships 3-1

3.1 Background 3-1

3.2 Summary 3-2

3.3 Observations 3-3

3.3.1 Disparity in Staff Size 3-3

3.3.2 Responsibility Fragmentation 3-3

3.3.3 Organizational Misalignment 3-3

3.3.4 Decentralized and Inadequate Oversight 3-4

3.3.5 Lack of Collaboration 3-6

3.3.6 Lack of Individual and Line Management Responsibility, Authority, and Accountability 3-7

3.4 Recommendations 3-8

Section 4 Security Policy4-1
4.1 BACKGROUND....4-1
4.2 SUMMARY....4-2
4.3 OBSERVATIONS....4-2
4.3.1 Lack of Enterprise Vision....4-2
4.3.2 Lack of Collaboration in Policy Formulation and Implementation....4-3
4.3.3 Inadequate Staffing....4-4
4.3.4 Inconsistent Implementation....4-4
4.3.5 Documentation....4-5
4.4 RECOMMENDATIONS....4-6
Section 5 Cyber System Security....5-1
5.1 BACKGROUND....5-1
5.2 SUMMARY....5-1
5.3 OBSERVATIONS....5-1
5.4 RECOMMENDATIONS....5-4
Section 6 Counterintelligence....6-1
6.1 BACKGROUND....6-1
6.2 SUMMARY....6-1
6.3 OBSERVATIONS....6-2
6.3.1 Counterintelligence Organization....6-2
6.3.2 Counterintelligence Approach....6-2
6.3.3 CI Resources....6-3
6.3.4 Performance Measures....6-3
6.4 RECOMMENDATIONS....6-4
Section 7 Site Safeguards and Security Plans, Vulnerability Assessments, and Performance Testing....7-1
7.1 BACKGROUND....7-1
7.2 SUMMARY....7-1
7.3 OBSERVATIONS....7-2
7.3.1 Vulnerability Assessments....7-2

7.3.2 VA Performance Testing 7-8
7.4 RECOMMENDATIONS 7-13

Section 8 Protective Force. 8-1
8.1 BACKGROUND 8-1
8.2 SUMMARY 8-1
8.3 OBSERVATIONS 8-1
8.3.1 Staffing 8-1
8.3.2 Clearance Process 8-3
8.3.3 Training and Qualifications 8-3
8.3.4 VA and PF Coordination 8-5
8.3.5 Response Plan Effectiveness 8-5
8.3.6 Target Folders 8-6
8.3.7 Chemical and Biological Weapon Defense 8-7
8.3.8 Central Alarm Station Alarm Rates 8-7
8.3.9 Recapture, Recovery, and Pursuit 8-7
8.4 RECOMMENDATIONS 8-9

Section 9 Security Incidents and Inquiries 9-1
9.1 BACKGROUND 9-1
9.2 SUMMARY 9-1
9.3 OBSERVATIONS 9-1
9.3.1 Inconsistent Incident Categorization 9-1
9.3.2 Redundant Reporting Systems 9-3
9.3.3 Inadequate Incident Inquiries and Report Review 9-3
9.3.4 Inadequate Tracking and Communication 9-4
9.3.5 Inadequate Security Incident Metrics 9-6
9.3.6 Inconsistent Infraction Administration 9-7
9.3.7 Inadequate Inquiry Resources 9-7
9.4 RECOMMENDATIONS 9-8

Section 10 Design Basis Threat Implementation 10-1
10.1 BACKGROUND 10-1

10.2 SUMMARY 10-2
10.3 OBSERVATIONS 10-2
10.3.1 Insufficient Collaboration and Guidance 10-2
10.3.2 Inconsistent Site to Site DBT Implementation 10-3
10.3.3 DBT Implementation Resources 10-4
10.4 RECOMMENDATIONS 10-4

Section 11 Security Research and Development Programs 11-1
11.1 BACKGROUND 11-1
11.2 SUMMARY 11-1
11.3 OBSERVATIONS 11-1
11.4 RECOMMENDATIONS 11-3

Section 12 Nuclear Materials and Waste Storage 12-1
12.1 BACKGROUND 12-1
12.2 SUMMARY 12-1
12.3 OBSERVATIONS 12-1
12.3.1 SNM Consolidation 12-1
12.3.2 Underground Storage 12-2
12.3.3 Protection of Radiological Material 12-3
12.4 RECOMMENDATIONS 12-3

Section 13 Security Resources and Requirements 13-1
13.1 BACKGROUND 13-1
13.2 SUMMARY 13-2
13.3 OBSERVATIONS 13-2
13.3.1 PPBE Implementation 13-2
13.3.2 Security Funding 13-3
13.4 RECOMMENDATIONS 13-4

Section 14 Security Contracting 14-1
14.1 BACKGROUND 14-1
14.2 SUMMARY 14-1
14.3 OBSERVATIONS 14-2

14.4 RECOMMENDATIONS 14-4

Section 15 Past Studies 15-1

15.1 BACKGROUND 15-1

15.2 SUMMARY 15-1

15.3 OBSERVATIONS 15-1

15.4 RECOMMENDATION 15-2

Bibliography 1

Appendix A. Security Plan Status

Appendix B. Past Studies

Figures

Figure 3-1. NNSA Organization 3-3

Tables

Table 13-1. Process Alignment with Program Management 13-2

Section 1
Introduction

1.1 BACKGROUND[1]

Since President Franklin Delano Roosevelt created the American nuclear weapons program by informal directive in October 1939, preserving nuclear security has been a national imperative. It also has been an exceptional challenge. Many of the difficulties inherent in nuclear security—creating an open yet secure atmosphere for world-class nuclear weapons science, managing contact with foreign scientists, securing and accounting for minute quantities of special nuclear materials—have been part of the program since its birth. Modern technology keeps bringing new challenges. Cyber security is one example; the proliferation of microelectronic devices—cellular telephones, personal data assistants, increasingly powerful laptop computers, and high capacity computer memory devices—is another.

Federal oversight of the nuclear weapons program has evolved through the years, beginning with the Uranium Committee in late 1939; transitioning to the National Defense Research Committee, then the Office of Scientific Research and Development, and then the Manhattan Project during World War II; residing in the newly created Atomic Energy Commission (AEC) in 1947; transferring to the Energy Research and Development Administration in 1975; and finally shifting to the newly created Department of Energy (DOE) in 1977.

In 1999, Congress, reacting in part to security lapses, transferred responsibility to a semiautonomous agency, the National Nuclear Security Administration (NNSA). Section 3212 of NNSA's Title XXXII legislative charter gave the NNSA Administrator authority over, and responsibility for, all programs and activities of NNSA, including safeguards and security (S&S). In practice, although NNSA is closely involved in security policy development, separate DOE offices outside NNSA develop security policy and conduct independent security audits and inspections.

Nuclear security, always important, has become even more critical in the after-math of September 11. NNSA is reorganizing its structure and its approach to managing the contracts for its government-owned nuclear facilities it supervises. A former commission highlighted a problem in the entire nuclear weapons complex—the aging federal and contractor scientific and technical workforce—which also pertains to the

[1] Because it also pertains to this study, we included the entire "Background" subsection from the following report: NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

approximately 150 federal security professionals in NNSA[2]. In 2002, another commission report identified the new challenges facing DOE in operating premier scientific institutions in the 21st century in a manner that fosters scientific excellence and promotes the missions of the Department, while protecting and enhancing national security[3]. Finally, a series of well-publicized security incidents had, by the summer of 2003, led Energy Secretary Spencer Abraham to direct NNSA to aggressively and broadly improve nuclear security.

1.2 APPROACH

Against this background, NNSA Administrator Linton Brooks established two groups to assess long-range issues affecting security management and protection.[4] The first study analyzed the federal security workforce;[5] this study, broader in scope, examines a multitude of factors that affect NNSA's security program.

For the past 18 months, we have independently reviewed security at NNSA sites. This report describes our analysis, summarizes our findings, and recommends ways to improve NNSA's security. We interviewed professionals who directly manage and indirectly support the security programs throughout the NNSA complex, including those at Los Alamos, Pantex, Oak Ridge, Livermore, Sandia, Nevada, and Savannah River and DOE and NNSA headquarters. We also reviewed past reports and numerous other documents relating to the nuclear security pro-gram and received briefings on topics germane to this study from responsible officials in DOE and NNSA.

We were given a very broad charter to take a strategic look at how security within DOE/NNSA is organized and structured, the interrelationships between various security disciplines, and the existing security policies, procedures, and practices in place to recommend possible improvements. We were specifically not chartered to look at specific security incidents and individual NNSA organizations in isolation.

---

[2] The Commission on Maintaining United States Nuclear Weapons Expertise was created pursuant to the National Defense Security Acts of 1997 and 1998 and delivered its report to Congress and the Secretary of Energy on March 1, 1999. The chairman of that commission, retired Navy Admiral Henry G. Chiles Jr., also directed the companion study on nuclear security personnel expertise (see Note 1).

[3] The Commission on Science and Security, chaired by former Deputy Secretary of Defense John J. Hamre, delivered its report, *Science and Security in the 21st Century*, to the Secretary of Energy in April 2002.

[4] National Nuclear Security Administration, "NNSA Announces Security Initiatives for Weapons Laboratories," Press Release, July 8, 2003.

[5] See Note 1.

1.3 REPORT ORGANIZATION

We begin the study by describing the culture of security at DOE and NNSA. We then describe the roles, responsibilities, and relationships of various security organizations and the security policy that governs them. We then discuss, in order,

- cyber systems security;
- counterintelligence;
- site safeguards and security plans, vulnerability assessments, and performance testing;
- protective forces;
- security incidents and inquiries;
- design basis threat implementation;
- security research and development programs;
- nuclear materials and waste storage;
- security resources; and
- security contracting.

We then close with a brief discussion of past studies concerning NNSA security.

Section 2
Culture

2.1 BACKGROUND

Previous studies of DOE have repeatedly criticized its cultural approach to security. In 1999, the President's Foreign Intelligence Advisory Board (PFIAB) found that DOE and the weapons laboratories have a "deeply rooted culture of low regard for and, at times, hostility to security issues."[1] The long-standing culture of the DOE organization affects NNSA security practices at all levels, from the enterprise to the individual.

In February 2002, NNSA's *Report to Congress* detailed the agency's plan to "integrate security and counterintelligence into NNSA Mission Activities."[2] In fact, NNSA has accomplished many of its stated goals in this area, but its culture still reflects many of the long-standing negative attributes of DOE. As a relatively new agency, NNSA has had little time to develop a unique culture, and its semi-autonomous nature makes changing the culture—to institutionalize security as integral to mission and individual responsibility—difficult.

2.2 SUMMARY

NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission:

- Lack of a team approach to security
- Disparate views and an underappreciation of security across the enterprise, such that security is not fully embraced as integral to mission
- Ingrained organizational relationships that inhibit an enterprise approach to security
- A bias against training
- An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards

[1] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.
[2] National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the NNSA*, February 2002.

- Lack of trust in the security organization
- An absence of accountability.

2.3 OBSERVATIONS

2.3.1 Lack of Team Approach

Complex-wide, the views of security are many and varied. The DOE/NNSA white-collar professional and managerial ranks tend to underappreciate it. The security culture in the production environment differs from that of the scientific and research community; production sees security as an integral part of the mission, and the researchers tend to see it as an additional or contracted service. Thus, DOE/NNSA has no team approach to security, instead struggling to succeed in an atmosphere of conflicting viewpoints, e.g., headquarters versus the field, lab versus lab, site office versus contractor, academic versus operational, union versus management, and non-NNSA elements of DOE.

This divisiveness—stemming from the strong cultural identities of the individual sites and lack of team approach—impedes effective security enterprise-wide. This cultural framework is reinforced by the lack of a career development and rotation plan, which promotes remaining in a single organization rather than taking a wider, more diverse range of assignments[3]. As a consequence NNSA tends to view security issues as site-unique rather than addressing their complex-wide implications.

2.3.2 Cultural Opposition

Numerous reports have criticized DOE security management, and repeated attempts at reform have failed or faltered. Congressional micro-management, geographic decentralization, layers of bureaucracy, frequent changes in leadership, low morale, competition among the laboratories and sites, and an inherent tension between the openness of scientific inquiry and need for governmental secrecy have all been cited as contributing causes. However, underlying these factors is the low regard for security—set in a deeply rooted culture of ingrained behavior, attitudes, and values—which has permeated DOE for many years.

The PFIAB report of 1999 saw "a department saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial."[4] Elements of that cultural environment persist today and significantly restrict NNSA's ability to institutionalize a different cultural environment, where security is valued as integral to mission.

---

[3] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

[4] See Note 1.

The ingrained cultural environment and long-established organizational relationships within DOE/NNSA inhibit an enterprise approach to security:

- The sites have historically enjoyed significant autonomy and are reluctant to surrender this independence for a more centralized approach. A common saying that reflects this field-to-headquarters relationship is "Negotiations begin when the order is issued."

- The fragmented and stovepiped security process within DOE/NNSA has resulted in a lack of process ownership and accountability, which complicates NNSA headquarters' assertion of centralized authority.

DOE/NNSA has tried to "manage the contract and not the contractor" to avoid micromanagement, but, under this philosophy the organization views its day-to-day oversight responsibility in a narrow contractual frame of reference rather than a broader national security one.

The NNSA-stated philosophy that headquarters will develop the "what" (security policy) and the field will develop the "how" (security policy implementation) reflects both the strong autonomy of the individual sites and NNSA headquarters reluctance to assert a stronger day-to-day oversight role.

The stovepiped culture and lack of sufficiently trained and qualified security professionals (as cited in Chiles report) promotes an overreliance on compliance checklists, rather a broader, more balanced focus on meaningful performance objectives.[5] This culture, and the overly bureaucratic organization, also limits staff members' understanding and appreciation of the broader security program objectives and their role in achieving them.

2.3.3 Bias against Training

A bias against training is evident, stemming from:

- an older workforce that believes training is more appropriate for younger recruits,

- inadequate training budgets,

- poor quality training, and

- lack of training relevance to job assignments.

The Office of Independent Oversight and Performance Assurance (OA) acknowledges the lack of white-collar security training and the need for a "security community."

[5] See Note 3.

2.3.4 Lack of Trust

Employees lack trust that the DOE/NNSA security organization is capable of dealing forthrightly, expeditiously, and responsively with security issues. As a consequence, they have a greater propensity than those in other organizations (such as DoD) to use alternative channels (such as leaking to media or seeking whistle blower protection) as a first course of action, rather than relying on the normal chain of command for resolution.

As noted in the Commission on Science and Security report[6]

> Two competing forces within DOE tear at the delicate fabric of trust among scientists, laboratory management, security professionals, and field and headquarters officials. The first is the inherent tension between the interests of science and the interests of security. The second force is the long-standing tension between headquarters and field elements. Managers and staff at headquarters question whether they can trust the systems that the laboratory directors create. Laboratory directors do not feel that they can always trust headquarters to back them up when security problems arise that could benefit from mutual problem solving...
>
> Trust is reciprocal. Employees need to trust their supervisor to manage a security system that protects them. This entails appropriate verification. Once an individual has earned trust, through the granting of a security clearance, that person should in fact be trusted. Yet that trust must be periodically verified. One must never lose sight of the fact that sometimes trust is misplaced, and the system must be able to effectively handle that inevitability. Trust must be embedded in a system that is designed to deter and prevent betrayal and, failing prevention, that provides for early detection.

2.3.5 Absence of Accountability

Historically, security responsibility within DOE/NNSA has been spread thin and is fragmented. There is no single proponent under the Secretary of Energy who "owns" the security process and ensures consistent application of security standards. Headquarters views security as primarily a field responsibility. Responsibility for security is diffused among a number of stovepiped organizations. This institutionalized fragmentation results in weak integration of security programs and functions. Roles and responsibilities have not been clarified to ensure security is embedded as a line management and individual responsibility. Many line and program managers do not view security as integral to their mission.

[6] Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*, John J. Hamre, Commission Chair, Anne Witkowsky, Project Director, April 2002. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

Diffused responsibility undermines meaningful accountability. There is a reactionary cultural approach to security which relies on external reviews and audits rather than internal management oversight and critical self-assessment to drive the security agenda. Lack of accountability breeds weak follow-up on identified security deficiencies which in turn breeds further external reviews.

2.4 RECOMMENDATIONS

1. Continue to promote greater collaboration and team building within NNSA with the goal of an enterprise approach to security. Support the Chiles panel recommendations on improved career development, assignment rotation training, professional qualification and certification, etc.[7]

2. Establish a more extensive security training program designed for white-collar professionals.

3. Make an unequivocal commitment to upgrade the quality, relevance, and ownership of security training programs and professional certification.

4. Emphasize a balance of compliance and performance objectives designed to incentivize and embed security improvement throughout NNSA, as part of an enterprise approach to security.

5. Create a stronger climate of trust in the security program. Differentiate honest human security errors from malicious, grossly negligent ones.

6. Adopt a more proactive approach to security through stronger accountability. Promote greater ownership of security through clarified roles and responsibilities, greater emphasis on security in performance assessments, and increased reliance on healthy self-assessment programs.

[7] See Note 3.

Section 3
Roles, Responsibilities, and Relationships

3.1 BACKGROUND

Congress established NNSA in March 2000 as a separately organized semi-autonomous agency within DOE,[1] to maintain and enhance the safety, reliability, and performance of the nation's nuclear weapons; maintain the nation's ability to design, produce, and test nuclear weapons; prevent the proliferation of weapons of mass destruction; and design, build, and maintain naval nuclear propulsion systems.

The enabling statute established a Chief, Defense Nuclear Security (CDNS), reporting directly to the Administrator, to implement security policies directed by the Secretary and Administrator and develop and implement security programs for NNSA. Separately, the Office of Safeguards and Security Programs (NA-55), reporting to the Associate Administrator for Infrastructure and Security, was charged with overall coordination and implementation of NNSA security programs.

In May 2003, NNSA issued its first *Functions, Responsibilities, and Authorities Manual* (FRAM) for safeguards and security (S&S).[2] The manual assigns responsibility to NNSA headquarters, the service center, or site offices for various aspects of S&S policy, oversight, approval, program management, financial management, survey, and training.

On December 4, 2003, DOE established a new Office of Security and Safety Performance Assurance (SSA), which reports directly to the Secretary and develops and implements the Department's S&S policies.[3] DOE tasked SSA with working closely with NNSA,

- through the Office of Security Policy (SO), to ensure that NNSA security policies align with Department security policies, and

---

[1] Title 32 of the National Defense Authorization Act for Fiscal Year 2000 (Public Law 106-65) created NNSA. The National Defense Authorization Act for Fiscal Year 2001 (PL 106-398) amended Title 32 to require additional information on NNSA's organization, planning, program-ming, and budgeting.

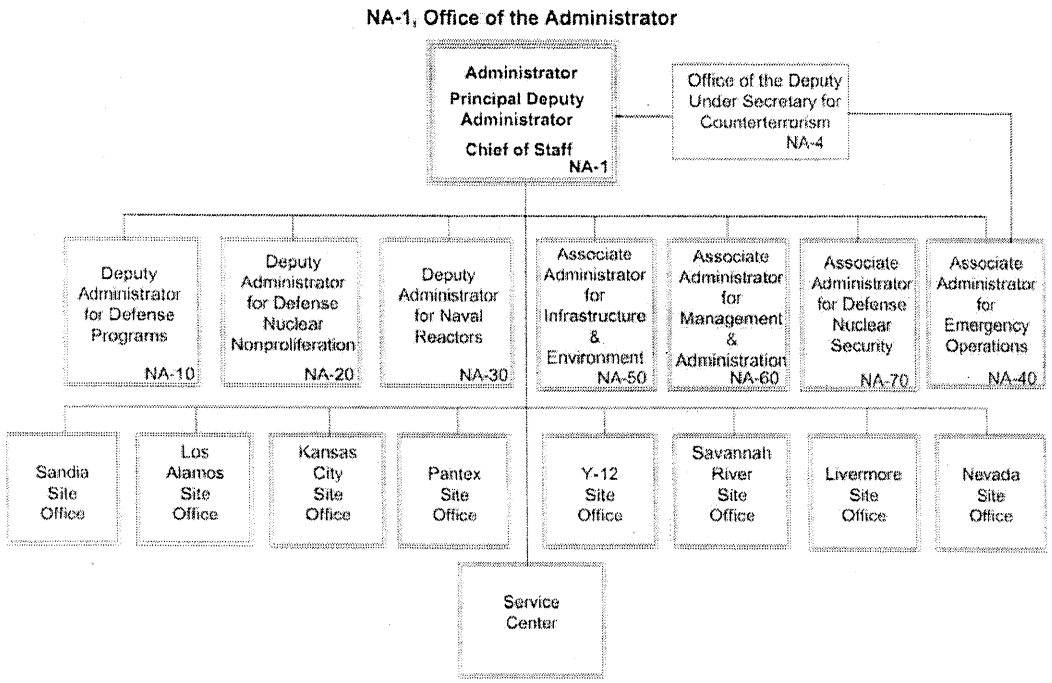
[2] National Nuclear Security Administration, *Functions, Responsibilities and Authorities Man-ual*, May 2003; Change 1, August 2003.

[3] U.S. Department of Energy, "DOE Establishes Office of Security and Safety Performance Assurance for Effective Implementation of Safeguards & Security Policies," *Press Release*, December 2003. Available from http://www.energy.gov/engine/content.do?PUBLIC_ID=14545&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE.

- through the Office of Independent Oversight and Performance Assurance (OA), to continue the independent oversight of NNSA's S&S, cyber security, environment, safety and health, and emergency management pro-grams.

In June 2004, during this study, the Administrator consolidated the CDNS and the NA-55 NNSA security functions into one office under the management of a new office of Associate Administrator for Defense Nuclear Security (NA-70). The cyber security function moved from the former NA-55 to the Office of the Chief Information Officer (NA-65). Figure 3-1 shows the new NNSA organization.

Figure 3-1. NNSA Organization



3.2 SUMMARY

The small size of the NNSA organization greatly impedes its effectiveness within the DOE headquarters bureaucracy. Although NNSA has made good progress by consolidating security functions, responsibility for security as a process is still fragmented and, along with authority and accountability for security, is not adequately embedded in individual and line management responsibilities. Until recently, staffs were organizationally misaligned. As identified in the Chiles report, security personnel with sufficient certification, training, rotation, and broad experience are lacking.[4]

[4] j NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Inde-pendent Analysis*, Henry G. Chiles Jr. et al., March 2004, pp. 2-3 and 2-4

Security collaboration between DOE/NNSA and DoD and among individual security disciplines is lacking. NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, effectively divorcing itself from day-to-day oversight.

3.3 OBSERVATIONS

3.3.1 Disparity in Staff Size

As the steward of the nation's nuclear stockpile, NNSA has a heavy responsibility, but the size of its organization is dwarfed by that of DOE overall. The NNSA portion of the FY05 budget request is $9 billion, or about 37 percent of the DOE FY05 budget request of $24.3 billion. However, the NNSA staff size is about 10 percent of DOE's. This disparity greatly impedes its effectiveness within the headquarters bureaucracy. For example, DOE SO and NNSA share responsibility for security policy, but, due to the staff size disparity, SO predominates in policy development. The disparity is even more skewed when one considers the large number of headquarters contractors employed by DOE relative to NNSA. Ironically, despite the current disparity in the staff size, NNSA was in the final phases of a 17 percent workforce reduction during the study period.

Beyond these overall numbers, as identified in the Chiles report, qualified security personnel—with sufficient certification, training, rotation, and broad experience—are lacking. Both headquarters and the site offices lack security depth and competency.[5]

3.3.2 Responsibility Fragmentation

Responsibility for security as a process is fragmented within DOE/NNSA. No single person beneath the Secretary has overall responsibility for the security process from policy formulation to implementation and oversight. Security policy is formulated predominantly outside of NNSA. NNSA headquarters has insufficient qualified people to conduct oversight reviews of site security organizations. As a consequence NNSA relies heavily on OA for support. The lack of security process "ownership" contributes to a lack of accountability within the DOE/NNSA security disciplines. As a result of diffused responsibility, a large DOE headquarters bureaucracy, and a turf-oriented culture, decision-making is often consensus driven, compliance based, and unresponsive.

3.3.3 Organizational Misalignment

The Office of Safeguards and Security Programs (NA-55), since realigned, lacked true line management authority, appropriate security expertise, and meaningful security responsibility. This organizational alignment did not serve

NNSA well and inhibited the day-to-day awareness of key security issues and concerns among senior DOE/NNSA decision makers. Elevating NA-55 to the Associate Administrator for Defense Nuclear Security (NA-70) is a step toward achieving increased NNSA security staff access and influence with senior DOE/NNSA leadership.

As discussed in Section 5, the head of NNSA cyber security was inappropriately assigned to NA-55 under the physical security experts rather than working directly for the NNSA CIO equivalent. This organizational alignment inhibited the development and integration of cyber security policies and implementing guidance with information technology policies.

3.3.4 Decentralized and Inadequate Oversight

NNSA headquarters has inappropriately delegated virtually all security oversight, review, and assistance responsibilities to the site offices, effectively divorcing itself from day-to-day oversight. The FRAM assigns an overwhelming majority of oversight functions—123 of 165—to the site offices; however, the site offices generally do not have enough appropriately qualified or certified personnel to perform this function effectively.

NNSA's ability to exercise comprehensive, day-to-day security oversight—to monitor security policy implementation, provide critical guidance and advice, assist in the identification of deficiencies and initiation of corrective action, and promulgate lessons earned and best practices across the enterprise—is problematic for a number of reasons:

- Security expertise is lacking at all levels of the oversight process.[6] Personnel with limited security experience and expertise accomplish much of the day-to-day oversight. For example, NNSA headquarters does not have sufficient oversight expertise for protective force, material control and accountability vulnerability assessments (VAs), and personnel security.

- As highlighted in a 1998 report, the oversight of nuclear weapons security is "a shared responsibility which encompasses numerous assumptions, offices, and echelons of management."[7] This diffused responsibility creates confusion and results in a lack of clear authority and accountability. For example, NNSA headquarters and many managers say that responsibility for site security oversight rests with OA. In reality, that office has little if any direct responsibility, authority, and accountability for day-to-day supervision of the NNSA complex. Its principal role is one of

[5] See Note 4.
[6] See Note 4.
[7] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf

periodic independent performance assessment. Although independent oversight is a necessary, integral function of NNSA's security organization, it is only a small part of an effective approach to security oversight. Other NNSA line managers believe that site oversight responsibility rests with the local site S&S offices and don't see security as integral to their supervisory responsibilities.

- The NNSA philosophy of centralized guidance and decentralized execution has evolved into a narrow interpretation of responsibilities described as, "headquarters does policy, and the field does implementation." NNSA has advocated decentralized day-to-day oversight without sufficient de-centralized resources. In effect, under this approach, NNSA has surrendered its responsibilities for day-to-day oversight to the field, which is inadequately manned and qualified to perform that function consistently and effectively. Additionally, the lack of centralized clarification of policy interpretation and centralized guidance on policy implementation impedes an enterprise-wide approach to security.

- The oft-quoted DOE/NNSA philosophy, "Manage the contract and not the contractor," has been narrowly interpreted by many NNSA officials to limit their oversight responsibilities to those of contract administrators.

- As a result of numerous outside influences (such as congressional mandates and independent reports), oversight responsibilities have been routinely realigned and modified. This regular restructuring has inhibited the maturation of cohesive oversight processes. For example, the effectiveness of the new Albuquerque Service Center has been hindered by "absentee leadership" (several key positions filled by people who do not reside in Albuquerque) and the unwillingness of employees of the field offices being disestablished to accept new positions and relocate to Albuquerque.

- Some oversight processes have been discontinued or fallen into neglect. For example, DOE's site safeguards and security plan (SSSP) validation and verification (V&V) process has been discontinued, so contractor vulnerability assessments (VAs) do not receive an independent external review. In addition, until recently, NNSA lacked sufficient resources to review the sites' incident reports of concern and verify appropriate corrective actions.

Effective oversight consists of several interdependent elements:

- Day-to-day line management oversight

- Periodic or continuous annual self-assessment survey programs

- Independent oversight.

These elements are intended to operate synergistically. In practice, however, they do not:

- Day-to-day NNSA oversight is lacking as described above
- NNSA guidance is vague on the administration of self-assessment programs. As a consequence, NNSA self-assessment programs vary widely in concept and quality. Self-assessment reports range from none to comprehensive. At present the safeguards and security self-assessment program can be characterized as marginally effective at most sites.
- The survey program has not lived up to its envisioned role. As federal and contractor staffs have been downsized, support for survey programs have diminished. The quality of both surveys and the analytical review of corrective actions have suffered. As a result, analysis of the root cause of deficiencies is often ineffective and corrective actions often address only the most obvious symptoms rather than correcting the underlying fundamental weaknesses. Weak survey programs tend to breed weak self-assessment programs.

3.3.5 Lack of Collaboration

Security collaboration between DoD and DOE/NNSA is lacking, despite the recommendations of a comprehensive independent review.[8] No formalized, established mechanisms exist for sharing security lessons learned, best practices, technological improvements, tactics, and procedures among the security organizations of the two departments.

Individual security disciplines—physical, cyber, personnel, material control and accountability (MC&A), intelligence, and counterintelligence—are not well integrated into a cohesive security program. Conceptually, the benefits of seamless integration are readily apparent. In reality, the various security disciplines do not sufficiently collaborate, despite their growing interdependence, and no single body within DOE oversees and integrates them. The lack of collaboration and cooperation, often results in uncoordinated, inconsistent, and, in some cases, vague or conflicting guidance.

The quality panel system, established to ensure maximum field element participation in and input to DOE security policy, is not effective. In general, there are too many panels (25 as of June 2004) for the sites to support, and the system has become excessively bureaucratic. The leadership of some panels is viewed by some members as "tyrannical."

Field assistance visits, which offered sites the opportunity to obtain policy clarification and other assistance from headquarters in a non-inspection format, have lain dormant for a number of years.

3.3.6 Lack of Individual and Line Management Responsibility, Authority, and Accountability

Responsibility, authority, and accountability for security are not adequately embedded in line management responsibilities. Security is not viewed as a mission-integral responsibility. In NNSA headquarters, the two principal program deputy administrators (NA-10 and NA-20) do not have significant direct responsibility for security, although they control almost all of the nuclear weapons program re-sources.

Additionally, many site, line, and program managers lack clearly delineated individual responsibilities for security. As a result, security is not viewed as an integral part of their mission, but rather as a service that others provide. Several factors contribute to this perception:

- The FRAM only focuses on safeguards and security staff and does not assign any significant security responsibilities to line and program managers.
- The fact that security is treated as a separate, direct-funded line item, administered separately from the stockpile stewardship programs also reinforces the perception that security is not integral to the programs and is often seen as a resource competitor.

In general, security falls into two categories: security common to all programs in a given facility (such as site perimeter security) and program-unique security. Line and program managers do not have sufficient responsibility for the program-unique elements of security. This separation of responsibility often impedes the ability of line and program managers to make appropriate resource allocation decisions to effectively administer their programs. Programs are often delayed because of security-related issues that line and program managers are not empowered to influence.

The Integrated Safeguards and Security Management (ISSM) program, was implemented in March 2001 for all NNSA federal and contractor offices and sites. The ISSM program was patterned after the successful Integrated Safety Management (ISM) program. As such, ISSM was designed to include core values and principles and rely on line management ownership of safeguards and security within their work scope, as well as individual employee commitment to conducting all work in a secure manner. ISSM was clearly intended to embed security as an individual responsibility; however ISSM was "stillborn." It has not been institutionalized into day to day management or embraced as an individual responsibility.

[8] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Secret).

3.4 RECOMMENDATIONS

1. Conduct an independent staffing assessment of NNSA relative to DOE. Rebalance staffing and expertise commensurate with the significance of the national security assets NNSA manages.

2. Give greater autonomy and authority to the NNSA Administrator to oversee the elements of the security process, from policy formulation to implementation and oversight, which directly affect security of the NNSA complex.

3. Implement the recommendations of the Chiles report to improve the federal security workforce, including developing and executing a comprehensive human capital management program; improving the training, qualifications, and stature of the NNSA security workforce; reengaging in national markets to hire security professionals; instituting a long-term practice of security staff rotation; identifying options for accelerating the security clearance process; improving security information flow; revising the *NNSA Safeguards and Security Strategic Plan*; and providing specific budget support for and tracking the progress of these recommendations.[9]

4. Continue to elevate security program visibility and importance through initiatives such as the June 2004 organizational realignment, to ensure security is commensurate with other line management responsibilities.

5. Have NNSA headquarters assume greater responsibility for day-to-day supervision and oversight of site activities to promote an enterprise-wide approach to security, more consistent interpretation of security policy, and more standardized and coherent implementation. The new Associate Administrator for Defense Nuclear Security should be assigned responsibility for day-to-day security oversight. Responsibility for implementation needs to reside at all levels.

6. Establish formal mechanisms to enable DOE/NNSA to regularly collaborate with DoD (and other appropriate federal agencies) on security policy issues, lessons learned, best practices, technological improvements, tactics, and procedures as recommended by a previous study.[10] This collaboration should be more frequent and at lower management levels than [REDACTED] the current guidance requires. The Nuclear Weapons Council may be an appropriate organization to sponsor this activity.

7. Establish forums and procedures to promote greater coordination and collaboration among the various security disciplines, such as the following:

---

[9] See Note 4.
[10] See Note 8.

- Consider establishing a security "board of directors" comprising NNSA prime security contractors and like-asset protection experts.

- Add to the responsibilities of the existing management council a requirement to convene periodic meetings to address security concerns. These meetings should include SSA, Counterintelligence (NNSA and DOE), Intelligence, CDNS, and the Cyber Security Manager.

- Consider establishing a DOE/NNSA security panel at headquarters and each NNSA site that requires key leadership representatives from physical security, cyber security, counterintelligence, and intelligence, as appropriate, to meet regularly to share knowledge and coordinate activities.

8. Embed greater security planning and programming responsibilities in the two Program Deputy Administrators (NA-10 and NA-70), for example, development of plans for consolidation of special nuclear material (SNM). Consider promoting greater line and program manager accountability for security by establishing a direct funding line to integrate the resourcing of program-unique security elements with their respective programs.

9. Streamline the quality panel system; reduce the number of panels, establish more discipline and a well-defined focus, and increase higher management participation to reduce bureaucracy.

10. Revitalize the ISSM program. (The NNSA Administrator has already taken action to implement this initiative.)

11. Promote greater reliance on continuing security self-assessment programs to better inculcate security as every individual's responsibility and integral to mission. Consider changing the annual survey and self-assessment program to a year-round program of in-depth assessments in specific areas.

Section 4
Security Policy

4.1 BACKGROUND

In May 2002, NNSA defined a formal system for development and codification of its policy, directives, and business management practices.[1] This policy letter system codifies how NNSA establishes policy and provides direction and guidance to all elements. The system establishes new policy for directives unique to NNSA, supplements or indicates how NNSA will cost-efficiently implement a departmental directive, and provides business and operating guidance. NNSA policy letters include directives, policy letters, and business and operating policy (BOP) letters.[2] The former describe "what" will be done, and the latter describe "how."

DOE develops and communicates its policies, requirements, and responsibilities throughout the Department by means of its directives system. The system informs, directs, and guides employees in the performance of their jobs, enabling them to work effectively within the Department and with agencies, contractors, and the public.[3] The five general types of directives are policies, orders, manuals, guides, and notices.

DOE Order 470.1 establishes the responsibilities, authorities, and requirements of the DOE Safeguards and Security Program.[4] Draft 470.1A, which has been distributed for review and comment, requires the Director, Office of Security, to establish "security policies, requirements, standards, and guidance, including the DOE Design Basis Threat (DBT) for use in designing and implementing the safeguards and security programs."

DOE vets policy by two methods—the Field Management Council (FMC) and the Review and Comment (RevCom) Process—before finalizing and distributing it:

- The FMC issues policy that has to get out to the field quickly. Since 1999, the FMC has taken 481 actions, 15 to 20 percent of which are security related. Although the actual council has not met since the Clinton Administration, DOE still employs the review process, which involves field sites and headquarters elements.

[1] NNSA defined this system under the authority of Section 3212(b)(2) of Public Law 106-65, the National Defense Authorization Act for Fiscal Year 2000.
[2] As of June 2004, NNSA had issued nine directives policy letters and eight BOP letters.
[3] U.S. Department of Energy, Office of Management Communications, "Department of Energy Directives Checklist," *Directives, Regulations, and Standards,* August 2004. Available from http://www.directives.doe.gov/cgi-bin/currentchecklist#POLICY.
[4] U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

- RevCom is the DOE coordination system for the development of administrative directives.[5] DOE employees and prime contractors use the system to comment on draft directives.

A July 2002 working group report stated,

> The Department's current coordination process is considered unnecessarily elaborate and bureaucratic by directives owners and customers. The group determined that the directives processed through the directives system during 2001 took an average of 295 days to coordinate and pro-vide the Deputy Secretary with a final directive for approval.[6]

In part, on the basis of this report, DOE's Office of Security and Safety Performance Assurance (SSA) is streamlining the Department's security policy. In March 2004, the Office of Management, Budget and Evaluation (ME) issued for comment a 1200-page draft on streamlining, and it plans to issue the final in fall 2004.[7]

4.2 SUMMARY

The NNSA enterprise lacks a comprehensive strategic security plan. Policy collaboration is lacking: between DOE and DoD, internally within DOE/NNSA headquarters, between headquarters and the sites, and among sites. NNSA does not have adequate staffing to direct policy to the field or facilitate site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in implementation. No effective system is in place for verifying documented security guidance and direction.

4.3 OBSERVATIONS

4.3.1 Lack of Enterprise Vision

The NNSA enterprise lacks a comprehensive strategic security plan that charts a course for the organization, strives to achieve better efficiency and effectiveness in security programs, and provides a unifying vision for the nuclear weapons complex.

---

[5] U.S. Department of Energy, Office of Management, Budget and Evaluation, *RevCom Re-view and Comment System*, August 2004. Available from http://www.revcom.doe.gov/.

[6] U.S. Department of Energy, DOE Directives System Working Group, Office of Management, Budget and Evaluation, *Report on Streamlining Directives System*, presented to the DOE Management Council, July 23, 2002

[7] ME issued the draft as Official Use Only (OUO), so it is not widely available for comment.

The Department of Energy's Strategic Security Plan is a well written document with 14 specific objectives[8]—divided into near, mid, and long term—with specific strategies designed to achieve desired intermediate goals and long-term outcomes. It also delineates qualitative and quantitative measures of success to assess progress toward meeting these objectives. In contrast, the *NNSA Safeguards and Security Strategic Plan* is more general, consisting of only 4 goals, which lack the specificity and the time frames of those in the DOE plan.[9] Although issued at about the same time, the two plans do not appear to be linked. The stark differences in the plans reflect a lack of collaboration between NNSA and DOE.

Of greater concern, the NNSA sites have adopted neither the DOE plan nor the NNSA plan. The safeguards and security plans of most NNSA sites reflect little linkage to either plan and vary widely in structure and content.

4.3.2 Lack of Collaboration in Policy Formulation and Implementation

Security policy collaboration between DOE/NNSA and DoD is lacking. The two departments differ greatly in their approaches to security policy and implementation.[10] No integrating process or overall management ensures the equivalence of their respective security approaches. At a minimum, the same nuclear weapon or material located within DoD or NNSA should be protected at an equivalent level against an equivalent threat on the basis of the intelligence community's postulated threat. As outlined in Section 10, this is not the case today. Prior drug use policy (peyote, for example) is also not standardized between DOE/NNSA and DoD.

Within DOE/NNSA headquarters, security policy formulation lacks appropriate collaboration. In general, SO formulates security policy, except for cyber security, which either the DOE Office of the Chief Information Officer (OCIO) or NNSA cyber security office formulates separately; collaboration between these offices is minimal. NNSA has little involvement with SO in policy formulation and interpretation, in part because of staffing limitations.

Appropriate security policy collaboration between the DOE/NNSA headquarters and field is also lacking. This has resulted in significant inconsistencies in policy interpretation and implementation throughout the NNSA complex. In recent history, DOE/NNSA had unnecessarily restricted SO from communicating with the field concerning the impact of safety and security policy on its operations. (Increased collaboration resulting from a recent DOE initiative to restore SO communication with the field should improve the formulation and implementation of effective

[8] U.S. Department of Energy, *The Department of Energy's Strategic Security Plan*, March 2003.
[9] National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003.
[10] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Con-trol System* (U), Final Report, April 2002 (Secret).

security policy.) The RevCom system also has not been effective as a collaboration tool; the sites perceive that headquarters does not consider their inputs.

Collaboration among sites is also lacking. Most sites perceive that early collaboration in the formulation of security policy is lacking.

Peer review is a critical element of the NNSA scientific process; yet, safety and security appear to be excluded from peer review. Although a number of forums and other groups have focused on security, they have not been effective in promoting meaningful collaboration.

4.3.3 Inadequate Staffing

NNSA does not have adequate staffing to direct policy to the field and to address, clarify, and interpret policy to facilitate site implementation. It also does not have the experience and expertise needed in key security disciplines, such as vulnerability assessments (VAs), to assist the field. Because of staffing limitations, NNSA has little effective involvement in policy formulation and interpretation.

4.3.4 Inconsistent Implementation

NNSA has not provided sufficient clarification and interpretation of security policy to facilitate more consistent site-to-site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in policy implementation. One headquarters employee stated, "Policy which is issued is not the best policy that can be written; it is the best policy that can be negotiated."

The prevalent philosophy of centralized guidance and decentralized execution, while commendable in purpose, suffers from a lack of centralized collaboration and clarification of policy intent, insufficient decentralized oversight expertise (at the site offices), and lack of enterprise standards and criteria. The abolishment of a previously effective security standards and criteria manual, and decentralized interpretation, undermine consistency of policies. Examples are as follows:

- Security policy on chemical and biological defenses is not well defined, particularly in regard to use of protective suits and gloves, (which at one site at least are still in the warehouse).

- The focus on exit security policy (for items people take or send from a facility) is weak compared with entrance security policy (for items people bring into a facility).

- Sites have differing interpretations of fundamental concepts such as "critical facilities" and "nuclear threat" as discussed in Section 7.

As a consequence, no coherent NNSA-wide security standards and criteria exist and an enterprise-wide vision is lacking.

Local site security policies have proliferated through a reactionary approach to implementing headquarters policies that are subject to wide interpretation. In one site's perspective, "Security policy has 50 years of band-aids; the bureaucratic band-aids have become the problem." This situation has contributed to a compliance-based (checklist) approach to security policy implementation and oversight, rather than a risk-based approach focused on outcomes, which better ties compliance to mission performance.

The DOE security policy streamlining initiative is commendable, but it is still in review. Because the draft streamlining initiative document is OUO, it is not available electronically.[11] The lack of access means fewer staff members can review, comment, and ultimately follow the guidelines.

4.3.5 Documentation

DOE/NNSA has no effective system in place to ensure organizations or staff can verify they hold a complete, up-to-date file of all security guidance and direction. No database or centralized program (other than the quality panels) identifies current supplemental directives for field offices and contractors to ensure that applicable memorandums, order changes, and guidance are followed. No consolidated listing of all effective security policy guidance or direction is available to ensure appropriate accountability.

All DOE security directives are unclassified as a matter of policy (for reasons not fully understood). As a consequence, classified policy guidance or direction (such as the new DBT security requirements) has not been incorporated into the directives system, but issued in the form of policy memorandums or letters.

The SO initiative to consolidate all unclassified policy in CD format, including an umbrella document and seven underlying manuals, is a step in the right direction, but it does not fully integrate cyber security policy or classified policy.

[11] U.S. Department of Energy, *Identifying and Protecting Official Use Only Information*, DOE Order 471.3, April 2003.

4.4 RECOMMENDATIONS

1. Formulate an NNSA-wide strategic security plan, similar in level of detail and content to DOE's, to create a unifying security roadmap for the NNSA enterprise. Use this plan as a cornerstone for the creation of other interdependent enterprise-wide plans, such as special nuclear material consolidation, infrastructure recapitalization, technology investment, information systems modernization, and the foundation for individual security discipline plans (physical, cyber, personnel, and material control and accountability).

2. Establish effective, formal forums to:

   - promote greater DOE/NNSA-to-DOD, DOE-to-NNSA, headquarters-to-site, and site-to-site collaboration between security policymakers and policy implementers,
   - promote more consistent interpretation and application of security policy,
   - foster adoption of best practices,
   - help formulate a more coherent, NNSA-wide security plan,
   - institutionalize the principles of the ISSM initiative in daily practice (the NNSA Administrator has already taken steps to implement this recommendation), and
   - consider making peer review an inherent element of security policy formulation and implementation.

3. Review and streamline local site compliance-based quick fixes to ensure security oversight is appropriately focused on performance objectives.

4. Provide greater centralized clarification and interpretation of security policy to promote more consistent and standardized implementation. Consider repromulgation of a security standards and criteria manual. As part of this initiative:

   - establish more definitive policies for biological and chemical defenses, and
   - better balance entry and exit security policies (both cyber and physical) to deter inappropriate or illegal removal of items from sites as well as entry.

5. Periodically promulgate a consolidated listing of all effective security policy (directives, letters, memorandums, manuals, etc). Consider establishing a single, integrated (unclassified and classified, cyber and physical) directives system with appropriate distribution controls.

6. Consider clarifying the DOE Order 471.3 so that OUO information can be placed on the unclassified network.

7. Reconcile security policy differences with DOD such as the policy on the use of hallucinogenic drugs (e.g. peyote).

Section 5
Cyber System Security

5.1 BACKGROUND

The security of NNSA information systems is an integral element of its mission. The rapid advances in information system technologies and increasing reliance on electronic networks and media call for evolving cyber security policies that ensure adequate management, operational, and technical security controls.

NNSA is operating in a highly interactive environment of powerful computing devices and interconnected systems of systems across global networks. These systems cross a variety of boundaries—both federal and commercial. The complexity of these cross-connected systems and networks presents great security challenges for NNSA.

Much of NNSA information requires some level of protection. Loss or compromise of this information, whether held directly by NNSA or its contractors, could directly affect U.S. economic, environmental, and national security interests. Implementing a broad, comprehensive program of information assurance to satisfy the NNSA information security requirements is critical.

5.2 SUMMARY

DOE/NNSA cyber security policies, procedures, and practices are less mature than their counterparts in other security disciplines. NNSA is resource poor in terms of secure or classified networks and access terminals. Insufficient resources have been devoted to address many of its cyber security issues, particularly the insider threat. Cyber security implementation varies widely throughout NNSA because of the lack of an enterprise approach, inadequate funding, insufficient cyber security personnel and expertise, and inadequate collaboration among DOE and NNSA cyber security organizations. Cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. This stovepipe approach to security has hindered the development of a more comprehensive coordinated approach to securing NNSA information assets.

5.3 OBSERVATIONS

NNSA lacks sufficient classified voice (STU 3-like) and data (SIPRNet-like) network access terminals; thus, personnel transmit a large volume of very sensitive information via mail or unclassified networks, with only the key elements (which would make the information classified) removed. Significant potential vulnerabilities result from:

- outsider access to a large volume of sensitive, though unclassified, data, which can create a classified "mosaic," and

- inadequate secure voice and data network access terminals which force people to use unclassified media to address sensitive, though unclassified, matters or talk around classified subjects.

In general, DOE/NNSA cyber security has focused almost exclusively on network perimeter security (such as firewalls and intrusion detection), leaving inadequate cyber security safeguards against the insider threat. Sufficient resources have not been committed to internal security controls and monitoring to both deter and detect inappropriate activities; periodic performance assessments have primarily evaluated perimeter security at the expense of internal security controls.

Despite NNSA Policy Letter (NAP) 14.1,[1] which defines the NNSA Cyber Security Program, implementation varies widely across NNSA, perpetuated by a lack of consistent minimum standards, wide differences in policy interpretation by individual sites, and lack of collaboration among sites. Site-level cyber security program plans radically differ from each other due to this lack of standardized criteria. A lack of standardization inhibits an enterprise-wide approach to cyber security. As one consequence, NNSA has not comprehensively assessed the risk to its information systems end to end as required by FISMA.

Federal staffing of cyber security positions within NNSA is inadequate. At present, only two employees and two contractors in NNSA headquarters, supplemented by very limited cyber security expertise at each site, are responsible for day-to-day cyber security. Several sites have an extremely low level of federal cyber security expertise relative to the sensitivity of their mission.

DOE/NNSA lacks an effective cyber security training and qualification program. Many federal and contractor cyber security personnel lack IT security professional certifications, such as CISSP, CISM, and GSEC.[2] Additionally, many line and program managers are unfamiliar with the basic elements of an effective cyber security program.

DOE/NNSA lacks a consolidated, accurate inventory of their information systems. While some information systems are known to lack certification and accreditation, the accreditation of others is questionable in light of the professional qualifications of the site accrediting officers.

---

[1] National Nuclear Security Administration, NNSA Policy Letter 14.1, *Cyber Security Pro-gram*, September 2003.

[2] CISSP = Certification for Information System Security Professional; CISM = Certified Information Security Manager; and GSEC = Global Information Assurance Certification (GIAC) Security Essentials Certification

NNSA cyber security is not sufficiently integrated with other security disciplines, such as physical, personnel, material control and accountability, counterintelligence, and intelligence. Accordingly, determining whether the resource allocation between cyber and the other security disciplines is appropriately balanced to en-sure the highest priority vulnerabilities are being addressed is difficult. For example, some cyber security personnel perceive that their inputs were ignored during budget preparations because of overriding concerns with physical security funding.

Collaboration between NNSA and DOE headquarters in setting cyber security policy is lacking. As a consequence, the policy is fragmented and inconsistent. For example:

- DOE/NNSA has no standardized cyber security architecture or standards and criteria
- There is virtually no collaboration between NNSA sites and the DOE Cyber Security Office. (Although legislation prevents a DOE officer from directing an NNSA officer, it does not preclude collaboration.)
- The NNSA initiative to establish the cyber equivalent of a design basis threat (DBT) is a positive step. However, DOE has yet to accept or adopt this "cyber DBT" approach to the rest of the department
- The Office of Environmental Remediation and Waste Management (EM) and NNSA cyber security policies are not fully consistent.

Cyber security incident reporting policies have not been adequately integrated into the incidents of security concern program. At present, no meaningful metrics are available to NNSA leadership to monitor and assess cyber security performance.

In the NNSA scientific and research community, cultural resistance to implementation of, and adherence to, individual cyber security policies (such as configuration control, patch management, and root access control) is long-standing and unresolved.

Field cyber security personnel perceive the new cyber security directives, NAPS 14.1–14.11, as increasing the administrative workload with little corresponding increase in security protection.

NNSA cyber security management does not have a seat on key cyber security forums, such as the following:

- Committee on National Security Systems (CNSS), http://www.nstissc.gov/
- Information Assurance Technical Framework Forum (IATFF), http://www.iatf.net/
- The Center for Internet Security, http://www.cisecurity.org.

No one in DOE/NNSA headquarters is qualified and certified as a transient electromagnetic pulse surveillance technology (TEMPEST) technical authority to direct the telecommunication security programs for TEMPEST, communications security (COMSEC), and protected distribution systems (PDS).

5.4 RECOMMENDATIONS

1. Expand classified voice and data network access terminals throughout NNSA. Shift sensitive information to secure networks to the maximum ex-tent possible.

2. Devote more emphasis and cyber security resources to the insider threat. Implement an internal NNSA-wide network architecture and security policies, including:

   - more robust identification, authentication, and access controls
   - more robust audit trail, auditing, and archiving capabilities
   - automated patch management
   - 24×7 staff to monitor for abnormal and unusual network activity
   - improved security awareness, training, and education
   - improved contingency and incident response capability.

   In addition, expand the independent verification and validation program and performance assessment programs to better evaluate cyber safeguards against the insider threat.

3. Develop more consistent standards, guidelines, and procedures to promote a more integrated, comprehensive, uniform implementation of cyber security policies across the NNSA complex, including:

   - formulation of an enterprise cyber security program plan

- development of an enterprise architecture that encompasses all NNSA networks.

4. Assess NNSA's cyber security program end to end to clearly establish the interrelationships of information technology assets, threats, vulnerabilities, and safeguards.

5. Increase the number and professional qualifications of federal cyber security personnel across the NNSA complex. Require key federal and con-tractor cyber security personnel to achieve certain IT security professional certifications before or as part of their assignment to critical positions.

6. Require screening of all sensitive network system administrators as part of the Human Reliability Program.

7. Establish a white-collar cyber security training program to appropriately train key line and program managers.

8. Develop a comprehensive, accurate inventory of information systems and validate their certification and accreditation status. In the absence of appropriate site accreditation expertise, NNSA should centralize network accreditation to promote greater uniformity in information assurance and explicit acceptance of risk across the NNSA complex.

9. Better integrate cyber systems security with other security disciplines (as addressed in Section 3).

10. Establish a cyber security policy panel in DOE/NNSA headquarters to improve the consistency, specificity, and adequacy of cyber security policies within NNSA.

11. Fully integrate cyber security incident reporting into the incidents of security concern program and establish meaningful metrics to enable leader-ship to monitor and assess the NNSA cyber security program performance.

12. Encourage DOE to adopt the NNSA cyber DBT initiative and continue to refine this approach.

13. Increase NNSA's national-level visibility of national level information security issues through assignment of NNSA cyber security representatives as DOE representatives to the following forums (and others as appropriate):

- Committee on National Security Systems (CNSS), http://www.nstissc.gov/

- Information Assurance Technical Framework Forum (IATFF), http://www.iatf.net/

- The Center for Internet Security, http://www.cisecurity.org.

14. Establish a position within NNSA for a certified TEMPEST technical authority to support the NNSA chief information officer (CIO) and cyber security manager.

Section 6
Counterintelligence

6.1 BACKGROUND

As the repository of the crown jewels of our nation's nuclear secrets, the NNSA complex will continue to be a major target of foreign (friendly as well as hostile) government and terrorist collection activities.

The National Defense Authorization Act for fiscal year 2000 established the NNSA and, with it, an Office of Defense Nuclear Counterintelligence (ODNCI). The act also codified the existence of the DOE Office of Counterintelligence (OCI). For approximately a year following enactment, the Director, OCI, also served as Chief, ODNCI. Subsequent congressional action prohibited these dual responsibilities, and, as a result, the Secretary appointed a Chief, ODNCI, in October 2000.

Thereafter, DOE and NNSA tried to establish a clearly defined working relationship between the two counterintelligence offices, culminating in a secretarial policy memorandum.[1] The counterintelligence organizational concepts embodied in the memorandum established the two managers and a shared headquarters program staff approach, with DOE/OCI managing counterintelligence activities at DOE sites, and NNSA/ODNCI managing counterintelligence activity at NNSA sites.

The Secretary recently notified congressional committees that he wants to combine the two programs into the Office of Counterintelligence, within DOE, reporting directly to him. The congressional legislative process will determine the outcome of this proposal.

6.2 SUMMARY

The DOE/NNSA counterintelligence (CI) program suffers from a dysfunctional relationship between OCI and ODNCI, insufficient collaboration with the other security disciplines, lack of a proactive approach to protection of information, and insufficient emphasis on the insider threat. CI budget allocations do not appear to be aligned with program priorities. Finally, performance objectives designed to promote CI initiatives to deter, prevent, and preempt espionage activities are lacking.

---

[1] U.S. Department of Energy, memorandum from Bill Richardson, Secretary of Energy, to John T. Conway, subject: *Providing Revision 1 of the 2000-1 Implementation Plan*, January 19, 2001.

6.3 OBSERVATIONS

6.3.1 Counterintelligence Organization

The relationship between OCI and ODNCI is dysfunctional. Both the OCI and ODNCI managers agree that the offices should be combined. Coordination and collaboration among DOE/NNSA counterintelligence officials and DOE/NNSA intelligence and security officials is insufficient. For example:

- OCI has issued a large number of intelligence information reports to the intelligence community without coordination with ODNCI or the DOE Intelligence Office.
- OCI and ODNCI have not been adequately involved in red-teaming activities in the vulnerability assessment (VA), performance testing, and site safeguards and security plan (SSSP) processes to help NNSA sites:
  - assess how potential adversaries could exploit information, particularly from open sources, to plan attacks against site assets;
  - identify and mitigate vulnerabilities; and
  - improve the quality of protection strategies reflected in VAs, performance testing, and SSSPs.
- OCI and ODNCI were not adequately involved in the iterative site analysis (ISA) process.
- Most security and intelligence people interviewed criticized the counterintelligence program as a one-way receptor of information.

6.3.2 Counterintelligence Approach

DOE takes a reactive, investigation-based approach to counterintelligence rather than having a broad, comprehensive, and proactive philosophy designed to prevent, deter, and preempt foreign intelligence collection and espionage activities. The principal purpose of the counterintelligence program should be the protection of DOE/NNSA information rather than the successful prosecution of people who engage in activities on behalf of a foreign government or terrorist group. The existing approach narrowly focuses on investigating potential illegal activity and has as a principal measure of program success the number of active investigations open.

The existing program does not sufficiently emphasize protecting DOE information from the insider threat. For example:

- Red-teaming initiatives to determine how a potential insider threat could do the most damage to national security, prioritize potential vulnerabilities, and develop protection strategies are weak to non-existent.
- Polygraphs, computer searches, and other analysis and inspection techniques are not adequately utilized in a random (or even targeted) manner to serve as a deterrent.
- The counterintelligence program lacks sufficient cyber security expertise at headquarters to adequately oversee IT-based counterintelligence activities against the potential insider threat.

6.3.3 CI Resources

In general, the sites perceive that DOE/NNSA has devoted insufficient resources to a CI strategy of "defense in depth" which DOE envisions. The three nuclear weapons laboratories are specifically concerned with a "systemic failure to align CI budget allocations with program realities" and the inadequacy of budgetary resources allocated to their resident CI programs.[2]

6.3.4 Performance Measures

The counterintelligence *Program Inspection Standard* is very compliance oriented and does not adequately focus on performance objectives designed to deter, pre-vent, and preempt foreign government or terrorist espionage activities.[3]

NNSA lacks an enterprise-wide approach to contractor counterintelligence performance measures. The FY04 counterintelligence performance measures ODNCI delineated vary widely in both detail and scope among the NNSA maintenance and operations (M&O) contractors without appropriate justification. Federal site managers have apparently been given wide latitude in the formulation of performance measures, which are incorporated into the performance evaluation of the M&O contractors. The wide variation in counterintelligence contractor performance measures reflects both a lack of collaboration among NNSA federal site managers and a lack of centralized guidance from DOE/NNSA headquarters.

---

[2] Letter, from G. Peter Nanos et al, Laboratory Directors, to Kyle McSlarrow, Deputy Secretary, October 10, 2003.

[3] U.S. Department of Energy, ODNCI, *Program Inspection Standard*, March 2002. We understand that this standard is being revised.

Counterintelligence performance metrics focus almost exclusively on quantitative measures—such as the percentage and number of people receiving awareness training, percentage and number of intelligence information reports (IIRs) issued, and, particularly, the number of active investigations—as the measures of pro-gram success, without equivalent focus on the quality or effectiveness of those elements.

6.4 RECOMMENDATIONS

1. Reunify the OCI and ODCNI organizations in a single office. Because the preponderance of vital national security information foreign governments and terrorist entities seek from DOE resides within NNSA—and because of the gravity to national security of the loss of nuclear weapons information—strong consideration should be given to a merged office working directly under the NNSA Administrator.

2. Adopt a broader, more comprehensive, and proactive counterintelligence approach that gives primacy to deterring, preventing, and preempting foreign intelligence and terrorist espionage activities over investigation and prosecution of offenders.

3. Place greater emphasis on the insider threat through increased:

   - red-teaming to assess and prioritize potential internal vulnerabilities,
   - use of surveillance techniques (such as polygraphs and computer searches) to serve as a deterrent, and
   - cyber security expertise within the NNSA headquarters counterintelligence offices.

4. Improve coordination and collaboration among counterintelligence, intelligence, and various security disciplines across the NNSA complex to better integrate counterintelligence in red-teaming security activities, such as the ISA, VA, performance testing, and SSSP processes. Devote more resources to analyzing open-source information from potential adversaries' perspectives. Coordinate IIRs with the DOE Intelligence Office before their submission.

5. Independently validate the allocation of CI resources to ensure scarce resources are focused on the areas of greatest risk to national security.

6. Standardize the counterintelligence performance measures where appropriate for M&O contracts across the NNSA enterprise.

7. Develop counterintelligence performance metrics that enable DOE/NNSA leadership to better evaluate the quality and effectiveness of program elements

as well as quantitative measures. Add qualitative performance-related objectives to the counterintelligence program inspection standard to subjectively evaluate initiatives to deter, prevent, and preempt espionage activities.

Section 7
Site Safeguards and Security Plans, Vulnerability Assessments, and Performance Testing

7.1 BACKGROUND

The effectiveness of NNSA protective systems is supposed to be formally and regularly examined through the conduct of vulnerability assessments (VAs). A VA is a systematic evaluation process in which qualitative and quantitative techniques are applied to identify vulnerabilities and arrive at effective protection of specific assets, such as special nuclear material (SNM). To conduct such assessments, DOE uses a number of different DOE-developed VA software programs, tabletop analyses, and performance testing.

The results of these assessments are documented at each site in a classified document known as the site safeguards and security plan (SSSP). In addition to identifying known vulnerabilities, risks, and protection strategies for the site, the SSSP formally acknowledges how much risk the contractor and DOE are willing to accept.

The SSSP process, including the VA and performance-testing programs, serves as the foundation for protection of weapons and weapon grade materials in NNSA. These plans define risk to the most critical NNSA assets, influencing site protective posture and directly affecting the resources and funding allocated across the complex. Site-specific limited scope performance tests and force-on-force exercises help identify risks and influence the accuracy of VAs.

7.2 SUMMARY

A number of factors—the shortage of experienced VA analysts, increase in work-load resulting from the new design basis threat (DBT), lack of a comprehensive VA training program, overreliance on a few VA tools, and lack of a rigorous, institutionalized VA approach—detract from the validity and consistency of VAs across the NNSA complex. In addition, weaknesses and wide variations in SSSP limited scope performance testing and force-on-force exercises distort physical security assessments across the complex, promote a false sense of security in selected areas, and complicate prudent allocation of security resources to address potential vulnerabilities.

7.3 OBSERVATIONS

7.3.1 Vulnerability Assessments

INADEQUATE STAFFING AND SKILLS

NNSA has a shortage of VA analysts because of retirements, exits to consulting and higher-paying positions, reserve duty activations, and other reasons. Increased workload—stemming from the modified DBT, additional targets, VA policy changes, and analysis of security upgrades—exacerbates the shortage problem.

The experience and skills of VA analysts vary widely. The cadre of experienced, expert personnel available in NNSA to perform VAs is very small, so VAs are often performed by less experienced analysts, delayed, or not performed at all. As a consequence, sites are submitting budgets for costly security upgrades without the benefit of completed VAs, which can result in inadequate upgrades, upgrades exceeding needs, and inappropriate funding amounts.

DOE/NNSA does not have a mature, comprehensive VA training program. VA analysts new to the process are expected to make major decisions on system effectiveness and upgrades. In addition, they need training for numerous different responsibilities, including modeling that uses as many as a dozen different software programs.[1] Although the recent effort to train VA analysts complex-wide is a step in the right direction, its success hinges on a well-defined, institutionalized approach, which DOE/NNSA lacks.

At individual sites, the number and expertise of VA personnel is inconsistent with the work scope. For example, one site, which has only two inexperienced VA analysts, has more work than another site, which has 10 experienced VA analysts. These two analysts will have difficulty meeting the VA milestones required to support major construction projects, DBT implementation, and other needs.

INAPPROPRIATE RISK ASSESSMENT

Some NNSA sites are not appropriately assessing security risk. The *NNSA Safeguards and Security Strategic Plan* calls for revising VAs and SSSPs to ensure consistency with the new DBT, and it cites updated VAs, SSSPs, and site security plans (SSPs) as an indicator of success.[2] However, the risk associated

---

[1] These include Analytic System and Software for Evaluating Safeguards and Security (ASSESS), Joint Conflict and Tactical Simulation (JCATS), Joint Tactical Simulation (JTS), Adversary Timeline Analysis System (ATLAS), ASSESS Query Tool, Access Knowledge Database System (AKDBS), Antiterrorist (AT) Planner, radiological dispersal programs, chemical and bio-logical weapon (CBW) software, and blast effects software, such as Blast Effects Estimation Model (BEEM), Explosive Effects Analysis Software (Blast FX), Blast Effects for Internal Detonations (Blast X), and Conventional Weapons Effects (ConWep)

[2] National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003, p. 4.

with some VAs does not reflect current operations because the VAs are based on future security upgrades that are not yet operational or an SSSP has not been recently writ-ten, approved, and submitted. At some sites, VA analysts have submitted vulnerability assessment reports (VARs) to site offices based on a number of security upgrades that have not yet been implemented and with risk inappropriately defined as if these upgrades were fully operational.[3] Some site offices have inappropriately accepted risk on the basis of these misleading reports. Although analyzing post-upgrade risk is beneficial, official VA risk for a given site should reflect existing security conditions.

In contrast, some sites' VAs are outdated. They show an obsolete site configuration, based on a security posture and operations from years past, and lack the data—existing status of site operations, threats, and protective measures—to accurately assess prevailing risk. Some sites tend not to complete VAs unless an SSSP needs to be submitted and approved. Meanwhile, they routinely use these VAs for major security system and budgeting decisions even though they no longer accurately reflect the existing configuration or include newer threats.

In addition to the above concerns, the majority of NNSA sites have not submitted SSSPs for approval as required in the last 3 to 5 years, and thus, new DBT guidance has not been incorporated. (Appendix A shows the status of safeguard and security plans for the NNSA sites.)

The shortage of VA expertise and other resources, along with the greater workload stemming from the new DBT and upgrade analyses are principal reasons why these VAs are outdated. The discontinuance of the VA validation and verification (V&V) process, as discussed below, has also exacerbated this situation.

COMPLEX-WIDE INCONSISTENCY

The VA program—approach, process, rigor, and tools—is inconsistent complex-wide, primarily because adequate policy, guidance, and training are lacking. To some degree, the different VA approaches at each site appropriately represent varying geographies, missions, and other factors. Although site-specific differences are justified, rationalizing the foundations of the VAs is difficult: more standardization, consistency, and rigor is needed. Each site has a different approach to conducting VAs, and in most cases the full process is not documented at the site level, leaving any entity outside of each VA program on its own to interpret the process and method used. In addition, determining the justification for the different sites' bases for analysis is difficult because of the dearth of process documentation.

[3] Even if these not-yet-operational upgrades pertained to the current risk, NNSA will not know their effectiveness until they are performance tested, especially since some are procedural.

Examples of inconsistencies include the following:

- Some sites use the worst-case position of the protective force to determine their response force times (RFTs), and others use an average or 80th percentile.

- Some sites use "pictures in time" to help determine RFT data, and others don't.[4]

- Some sites heavily rely on a single VA software tool. For example, to determine the probability of neutralization, some sites use ASSESS BATLE only,[5] some use JCATS analyses only, and some use iterative site analysis (ISA) results. In other cases, where applicable exercises have been con-ducted, the sites have not incorporated results in the neutralization probability.

- Some sites rely on ISA as the primary method of identifying risk. [REDACTED]

ONE-TIME ISA PROCESS

In response to the events of September 11, 2001, the Chief, Defense Nuclear Security, developed the ISA process. It was designed to conduct site-by-site analyses of today's most realistic threats at the sites, as determined by a team of outside experts. It was a one-time event of great value—value that has yet to be duplicated by any other VA software tool or method when evaluating a single attack in depth.[6] Some sites want to continue to conduct ISAs and incorporate the results in their VA and SSSPs. However, NNSA has not disseminated guidance on incorporating the ISA process in the VA and SSSP, and additional ISAs have not been planned.

Although the ISA process takes a detailed approach in its evaluation of a single target, it is not designed to address all targets at a given site. The process is an

[4] Pictures in time are random, unannounced observations of protective force positions and configurations, which are duplicated during force-on-force exercises or JCATS analyses to ensure realism.

[5] The Brief Adversary Threat Loss Estimator (BATLE), an older computer model, was incorporated into ASSESS.

[6] This ISA process includes in-depth planning and information gathering meant to simulate the activities of real-world adversaries, such as collecting open source information for adversary attack planning, using active duty special operations personnel, and documentation of attack plans through an operations order format supported by real world combat experience.

"inch wide and a mile deep" in that it evaluates a specific target using a specific scenario. Other DOE/NNSA VA tools and methods tend to be more encompassing in analyzing a variety of threats and adversary scenarios to determine system effectiveness. The ISA process provides specific insights that other VA tools are not capable of providing, but other tools provide insights that ISA is not designed to accommodate. Two sites heavily rely on the ISA process as the foundation of their VA, without utilizing other VA modeling software; as a consequence they have incomplete target and scenario coverage.

JOINT CONFLICT AND TACTICAL SIMULATION (JCATS) ANALYSES INCONSISTENCY

The accuracy of the risk that sites are reporting is questionable. The inherent limitations of JCATS as a modeling tool, the lack of incorporation of exercise results in the probability of neutralization, the absence of existing standards and protocol rigor, and JCATS use as the sole tool for determining the probability of neutralization within the risk equation all contribute to this questionable accuracy.

The use of JCATS analyses varies complex-wide:

- Some sites use it as the sole method for determining the probability of neutralization.
- Some sites use a terrain file that only depicts the portion of the site to be analyzed instead of showing the entire menu of targets available to the adversary force. The limited JCATS terrain model alerts the protective force ahead of time as to which target will be attacked.
- JCATS software updates, reflecting the full weapons capabilities of the new DBT, are not centrally managed or issued to the sites. [REDACTED]
- Sites are increasingly using JCATS to dictate exercise scenarios, prohibiting the adversary force from deviating from the attack plan on the basis of the battlefield situation—thus negating its tactical advantage—because the change doesn't match the computer simulation.
- JCATS is not capable of analyzing some potential adversaries' weapons capabilities. As a consequence, some sites limit the adversary weaponry for exercises to match the weapon systems that can be evaluated by JCATS; thus, some DBT weapon capabilities do not undergo an evaluation by means of any performance test.
- Some sites have noted mistakes in the JCATS software terrain file. One site modeled a potential upgrade where a fence was used to simulate a

wall. Unknown to the JCATS system administrator, the fence allowed the protective force to shoot the adversary force through the fence when they would have realistically been behind a wall. In another JCATS analysis, instead of several adversaries traversing through the same breach point, each was required to breach a separate hole, adding an unrealistic delay time and putting the adversary force at a disadvantage.

Both exercises and JCATS have strengths and weaknesses; however, DOE/NNSA has not determined the extent to which they should be used to influence the probability of neutralization. DOE/NNSA has also not issued policy that provides each site a standard or minimum level of rigor for conducting exercises or JCATS analyses.

UNDERUTILIZED SOFTWARE TOOLS

DOE/NNSA has not provided guidance on the use of software tools in the VA process. Consequently, a number of tools developed by Sandia National Laboratory—such as AKDBS, ASSESS Query Tool, and ATLAS—are not being utilized in the field.[7] Blast effects software also has not been widely used; again, DOE/NNSA has issued no guidance regarding the standard to be used (such as AT Planner, Blast FX, Blast X, or BEEM).

INCONSISTENT CRITICAL SYSTEM ELEMENTS

NNSA lacks a standardized process for identifying critical system elements when conducting VA analyses. DOE Order 470.1 discusses critical system elements in general;[8] however, NNSA policy and guidance does not specify identification methods, testing methods, and how to incorporate test results in VAs. The sites' VAs identify critical system elements in broad terms and often do not identify all of them. The broad, general identifications make it difficult to determine the criticality of the item identified, such as protective force awareness. In other cases, testing focuses on protective force personnel and does not consider the two-person rule,[9] Personnel Security Assurance Program (PSAP), and other components of the protective system, which should be defined as critical.

INSUFFICIENT VA PROTOCOL DOCUMENTATION

Protocol documents that depict the sites' VA methods and processes are lacking.

---

[7] See Note 1.

[8] U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

[9] The two-person rule is a system designed to prohibit access by an individual to nuclear weapons and certain designated components by requiring the presence at all times of at least two authorized persons, each capable of detecting incorrect or unauthorized procedures with respect to the task to be performed. Source: http://www.dtic.mil/doctrine/jel/doddict/data/t/05538.html.

Some sites have operating procedures for conducting JCATS analyses, limited scope performance tests, and force-on-force exercises, but these documents fall short of identifying how rigorous or detailed the analyses should be. For example, a procedure might identify administrative assignments for force-on-force exercises (such as armorer issuance of MILES gear),[10] but it does not describe the difference between validation and training exercises, the minimum amount of time the adversary force has to plan its attack, how picture-in-time data are utilized, controller training requirements, or how weapon effects are controller called if the MILES gear systems are incapable of representing a certain weapon (such as 40 mm grenade launchers). Exercise protocol documents serve more rudimentary functions, such as (in the case of JCATS) describing the rotation of what is termed in DOE/NNSA a "puck" driver or setting the minimum number of JCATS runs to determine neutralization.

Sites that use JCATS results as the only method for determining the probability of neutralization do not have a documented process that identifies such actions as how picture-in-time data are incorporated in the JCATS analyses and whether each crew is tested.[11] For example, no protocols exist to prevent a site from using a mixture of selected protective force personnel from all the crews, which would not represent a single, site-specific operational protective force crew. The results of this type of analysis do not reflect each crew's capability.

Insider Threat Interpretation Variance

Interpretations of the insider threat under the new DBT differ from site to site, resulting in an inconsistent approach to VAs throughout the NNSA complex. An unclassified portion of the DBT defines an insider as someone who is unescorted. This wording has caused some NNSA sites to interpret someone who is escorted as not an insider and hence not requiring VA analysis. As a consequence, many non-PSAP insiders who were escorted have not been included in VA analyses.

[REDACTED]

Lack of VA Oversight

DOE/NNSA headquarters and site office VA oversight is lacking. The Chiles re-

[10] MILES (Multiple Integrated Laser Engagement System) gear enables force-on-force training through a system of lasers and sensors.

[11] See Note 4.

port, *Strengthening NNSA Security Expertise*, observed that the federal security workforce rated VAs as "highly important," but also stated, "Discussions pointed out the ability to expertly review and critique the contractor's vulnerability assessment as a particularly weak area of NNSA security personnel."[12]

The oversight of VAs also suffers from a conflicting perception of responsibility as well as a lack of resources. DOE has discontinued the SSSP V&V process. NNSA headquarters representatives have expressed a desire to review and approve site-submitted SSSPs, but they are not currently doing so. Within DOE/NNSA there is a fundamental disconnect in the understanding of the role of the DOE Office of Independent Oversight and Performance Assurance (OA) in the VA oversight process. OA conducts a relatively short VA review during its 18-month desired rotation inspection process for all DOE and NNSA sites. OA representatives stated that they do not extensively review site VAs during the OA inspection, that they don't fully validate VAs (only a sample thereof), and that OA should not be viewed as the organization that validates VAs. In contrast, NNSA representatives stated that they rely on OA for oversight of VAs.

7.3.2 VA Performance Testing

INCONSISTENT LIMITED SCOPE PERFORMANCE TESTING

Protocol documents delineating the method and process of site VAs and performance testing are either nonexistent or lack depth. Existing documents lack any detail regarding how tests are identified, approved, conducted, documented, and analyzed and thus are inconsistent across the complex. Very few limited scope performance testing programs have documentation that describes the evaluation of test results and their integration back into the VA process. Many tests do not provide the data that should be sought by the VA analysts.

The documentation that does exist is generally not intended for effectiveness testing but for operability testing only. For example, site personnel may test the operability of a set of alarm sensors—waving a hand in front of a motion sensor to ensure the alarm activates at the central alarm station (CAS)—but do not conduct tests that attempt to circumvent or spoof the alarm sensor.

The methods and processes for identifying and conducting limited performance tests, and integrating them into the VAs, are inconsistent and lack rigor. The

[12] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004, p. D-7.

strategic plan cites "Internal and Independent evaluations and performance tests document system performance and capabilities" as a success indicator.[13] However, the tests stop short of obtaining the most important pieces of site-specific performance data.

The tests conducted focus narrowly on the protective force instead of the two-person rule, PSAP, and other aspects of personnel adhering to procedure, which in some cases are more prone to failure because of their heavy reliance on the human element, as opposed to an automated sensor system. Tests that attempt to conduct an unauthorized activity to actually determine a site-specific probability of detection for various defeat strategies are almost nonexistent. When all DOE/NNSA site VAs are based on predefined detection probabilities within the various computer VA models used, there is little confidence in the accuracy of the risk reported if controlled, site-specific tests of unauthorized activities are never conducted.

Examples of other testing shortfalls are as follows:

- Some narrowly focused tests don't include critical elements or components of the protective system. For example, protective force alertness to detect airborne intrusion is excluded from evaluation when protective force supervisors, who were notified of a helicopter overflight in advance, are allowed to detect and report the intrusion.

- A site gives a 90 percent VA probability of detection credit to a specific protected area perimeter, but this same intrusion detection perimeter has 800 to 900 false and nuisance alarms per month.

- Most sites do not rigorously test adherence to the two-person rule, but rather simply observe whether the two people keep each other in line of sight. Tests designed to distract someone or simulate performance of an unauthorized activity to actually determine the probability of detection for various defeat strategies are practically nonexistent.

- [REDACTED]

- Tests measure how quickly a responder can traverse from point A to point B but fail to account for the time it takes to don fighting equipment or traverse the distance while under fire.

Because the VA software tools rely on these data, the inadequate testing results strongly influence the overall risk reported for each NNSA site.

[13] See Note 2, p. 4

INADEQUATE FORCE-ON-FORCE EXERCISES

Like limited scope performance testing, force-on-force exercises are inconsistent and lack rigor. It is not clear whether force-on-force exercises provide an accurate assurance of protective forces' capabilities to meet the new DBT because of several factors:

- exercise scenarios are constrained by many mandated restrictions such as routes of ingress/egress for safety, prescribed weapons and tactics
- adversary forces used in most of the force-on-force exercises are not fully representative of the new DBT
- NNSA lacks a testing regime similar to DoD's Mighty Guardian exercise program. Under this DoD program, a team of experts trained to think and act like potential adversaries and patterned on the postulated threat are used to evaluate DoD's nuclear security forces and protection strategies in free-play, realistic scenarios. The exercises are designed to stress forces to their limits while ensuring that the results are not treated as an inspection.

Insufficient distinction is made between DOE/NNSA exercises, designed to train people and explore new tactics and technologies, and evaluations that are designed to assess performance. In general, security force contractors are not incentivized to conduct rigorous exercises that really stress protective forces because the lack of a distinction between exercises and evaluations creates the potential of an exercise failure adversely impacting the assessment of contract performance. The pressure to not fail a force-on-force exercise inhibits useful training and promotes some inappropriate behavior. For example, some sites:

- identify administrative assignments but don't specify important practices or internal methods that significantly influence the exercise rigor and accuracy of the results
- conduct training exercises that are scaled down to the point that they don't test the overall protective system capabilities, instead of comprehensive validation exercises that do
- practice the exact exercise scenario just days before the exercise
- give the adversary force minimal time to plan its attack
- don't use a picture-in-time concept, detracting from the realism of the

starting point and configuration of the protective force[14]

- use the same crew, a combination of the best protective force members from all the crews, or selectively hire the protective force on an overtime voluntary basis (typically, the best qualified protective force members participate as volunteers) instead of rotating representative crews
- script the adversary's tactics to the point of predefining weapons, rather than letting the adversary force choose the weapons most advantageous for the scenario and terrain
- don't use exercise results to validate or otherwise influence the probability of neutralization reported in the VA because of sole reliance on the results of the JCATS computer simulations
- inconsistently use exercise (validation, training, stress exercises, etc.) results. For example, a site uses the results of a training exercise to support an assessment of low risk but omits validation exercises that may have resulted in negative outcomes.

Sites seldom use special operations personnel as adversary force team members during exercises, preferring to rely on their protective force personnel. For example, one site has refused to use "Grizzly Hitch" personnel as adversaries because, it perceives, they do not play fairly or by the rules proposed by the site.[15]

Although it is impractical to employ special operations personnel for most exercises, the use of protective force members in most cases can't duplicate the realistic operating experience associated with a professional adversary force. Exercises that use protective force personnel as adversaries often have unrealistic results because these personnel are primarily trained as defenders and lack experience in heavy weapons, explosives, airborne assets, etc. Continued overreliance on the use of protective force personnel as exercise adversaries—rather than more realistic terrorist planning and modus operandi unforeseen by the site—has the potential to create a false sense of security.

Some sites fail to comply with DOE policy, which requires at least one exercise quarterly. Some sites conduct several exercises over a year's time, falling short of the quarterly testing requirement. These situations stem in part from scheduled overtime and the manning of higher security condition levels, which have limited the availability of the protective force to train and participate in exercises. Interpretation and application of the quarterly exercise policy vary widely throughout the NNSA complex because of a lack of clear guidance. Some sites interpret "exercise" as a scaled-down test involving only a portion of the protective force and a less-than-full DBT adversary threat in a training setting; other sites interpret an exercise as a full-scale test involving an entire protective force crew and a full DBT adversary force.

[14] See Note 4.
[15] Grizzly Hitch is a trained intruder force drawn from DOD Special Operations community.

Because the quarterly exercise requirement doesn't specify how often each category I SNM facility is to be exercised, some sites conduct repeated exercises on the same target for years rather than testing a different on-site SNM facility.

The current quarterly testing requirement can contribute to an imbalance in the exercise frequency of the Category I SNM targets complex-wide. For example, site X has 50 different targets and site Y, only two. Each has the same exercise requirement. Site Y can exercise each category I SNM target several times per year, but site X takes much longer (many years) to exercise each target. Therefore, each site should rotate the types of targets that undergo an exercise to have a representative sample of the target set at each site; for example, sites should test various types of targets, varying them to test response and personnel that may be excluded if only a specific section of the facility continues to undergo an exercise.

Some sites need exercises that are more realistic. The "telegraphed" awareness that the site is about to be attacked (from an opened exercise window or a scheduled JCATS analysis) can tempt the protective force to assume a position or configuration that does not represent its day-to-day operations. To preclude this situation, a few sites capture pictures in time—a relatively new aspect of the VA process—as a verifiable method for determining protective force posture, armament, etc.[16] Security management may not know how the protective force is truly configured day to day. At present, the picture-in-time concept is one of the better methods of providing a semblance of realistic randomness, and sites can integrate it into the neutralization process, such as exercises and JCATS analyses, however it is not currently a DOE/NNSA requirement.

Many sites do not have pictures in time, raising concerns as to the accuracy of protective force positions for JCATS simulations or force-on-force exercises. When sites do use pictures in time, they often don't try to gather all the needed information—such as visiting the Central Alarm Station (CAS) to find out where the CCTVs are pointed or determining the locations of backup communication equipment (pagers and cellular telephones). Individually, these pieces of information may seem unimportant, but collectively they can significantly influence the overall protective system effectiveness. For example, not knowing the CCTV monitors that are observed within the CAS on a random basis makes it difficult to ensure the realism of detecting an adversary by CCTV in JCATS or during an exercise. Gathering all pertinent information ensures that realism and day-to-day operations are replicated in the testing process.

Training to one particular type of scenario also detracts from realism: although it may begin as a VA worst-case scenario, the more it is exercised, the less worst-case it becomes. When training and the response plan narrowly focus on a scripted scenario, slight variations can challenge the protective force.

[16] See Note 4.

7.4 RECOMMENDATIONS

1. Establish clear day-to-day oversight responsibility and accountability for the VA, SSSP, and performance testing programs within NNSA headquarters. Ensure plans and programs are current and reflect the new DBT. Periodically utilize OA resources to independently assess the performance of these programs.

2. Improve the recruitment and training of VA analysts, and balance VA expertise across the NNSA complex. Address the near-term shortage of VA expertise at selected sites through temporary reassignment. Continue development of a comprehensive VA program of instruction to:

   - better train and certify VA analysts
   - promote a more standardized VA method
   - foster greater knowledge of the strengths and limitations of various tools.

3. Develop policy and guidance for standardizing the VA, SSSP and performance testing processes and establishing more rigor and consistency across the complex. Develop standards that accomplish the following:

   - Document a consistent VA protocol.
   - Set a minimum level of rigor for all VA tools and methods used to define risk.
   - Limit the extent to which a single software tool can be used in determining the probability of neutralization and balance software tool usage with field-testing results (which require the entire protective system to actually perform). For example, provide guidance on using JCATS to complement performance testing results, not substitute for them. Use force-on-force exercises to contribute more to the foundation of a site's probability of neutralization.
   - Provide guidance for performance testing to help standardize how VA analysts identify protection elements and components that should be tested and how the results should be calculated and integrated into the VA process. Prepare detailed protocol documents for force-on-force exercises to capture the aspects—preplanning, conduct, and after-action tasks—that influence exercise realism and value.
   - Adopt true free-play, force-on-force testing for the exercise program, in which the threat force is not artificially limited in its ability to apply known terrorist tactics or weaponry. The threat force should routinely comprise expert adversaries, who, by their training and operational background, can think and act like terrorists.

- Clearly identify and delineate critical system elements and specify how the elements should be tested and the results incorporated into VAs, SSSPs, and performance testing

- Clarify the DBT policy related to the insider threat to ensure consistent interpretation.

- Provide policy and guidance to those responsible for identifying, writing, conducting, documenting, and analyzing VA performance tests to ensure a higher level of rigor and standards. Ensure that site exercise programs evaluate a broad range of components that span the site's protective system (detection, delay, and response force times), including insider-type defeat strategies (two-person rule, etc.).

- Establish policy and guidance for force-on-force exercises and their utilization in the VA process. Provide guidance that ensures each site is conducting exercises and JCATS analyses in a manner that precludes the protective force from intentionally or unintentionally knowing the adversary tactics, strategies, and target selection. Guidance will result in greater consistency and standardization among NNSA sites, including the rigor with which a validation exercise should be con-ducted and how exercise data can be used to support the site's probability of neutralization.

- Provide guidance on the use of the external special operations team (such as Grizzly Hitch) as the aggressor force or establish a trained aggressor force that does not comprise protective force members from the same site.

- Provide specific policy on the quarterly exercise requirement, including the degree to which different protective force crews and targets are tested. Provide a balanced policy approach, which requires rotation of exercised target areas to reflect the diversity of site-specific targets.

- Require pictures in times to be conducted for each site so that normal protective force configurations can be documented and serve as a preparatory step for force-on-force exercises and JCATS analyses.

4. Consider creating an NNSA-wide core VA team that routinely assists sites in the conduct of VAs and ensures a greater consistency and quality in VAs across the NNSA enterprise. The core team would also provide a mobile VA training function as it rotated from site to site.

5. Ensure that approved site SSSPs and the risk acceptance inherent in these SSSPs are based on VAs that evaluate existing operational conditions. Do not allow risk acceptance to be based on planned or projected security up-grades. Encourage sites to use the VA and SSSP process to analyze the effectiveness of potential security upgrades and project future risk.

6. Reinstitute the ISA process on a recurring basis in the conduct of VAs and development of SSSPs.

7. Promote more rigorous, realistic exercises that really stress protective forces (to understand their limits) by providing greater immunity to security contractors, such that exercise results are distinct from periodic performance assessments and do not affect contract performance.

8. Adopt a force-on-force exercise program for NNSA sites similar to the DoD Mighty Guardian exercise program, or expand the Mighty Guardian exercise program to include NNSA sites. Under this program, a team of experts trained to think and act like potential adversaries, patterned after the DBT, would conduct the exercises. NNSA would use the results of these exercises to rationalize past differences in DoD and NNSA performance testing and more accurately validate protection strategies.

Section 8
Protective Force

8.1 BACKGROUND

Each NNSA site hires and maintains its own protective force (PF) personnel to protect special nuclear material (SNM), classified material, and NNSA assets and employees. The PF, which includes approximately 2,400 officers nationwide, comprises several contractors and unions and is divided into the following categories:

- Security Officer—unarmed officers
- Security Police Officer I and II (SPO I and II)—armed defensive officers and offensive responders
- Security Police Officer III (SPO III)—special response teams (SRTs) and offensive responders.[1]

Each category of officers has its own physical fitness, weapons, and training qualifications.

8.2 SUMMARY

NNSA lacks a consistent approach for validating PF manning; because of wide variations in site approaches, determining whether site PFs can adequately meet the requirements of the new Design Basis Threat (DBT) remains problematic. PF performance is degraded by an excessive backlog in security clearances, inadequate guidance and training in several significant areas (such as adversary pathways, chemical and biological weapon defenses, and recapture, recovery and pursuit), and a lack of collaboration with vulnerability assessment (VA) experts, FBI, and local law enforcement officials. Response plans, target folders, and central alarm station systems need upgrading to improve PF readiness.

8.3 OBSERVATIONS

8.3.1 Staffing

PF staffing is not based on clear, well-defined policies and a consistent NNSA-wide methodology. Although the NNSA strategic plan states, "We will use a systems

[1] We did not visit the Office of Transportation Security, which consists of federal officers

engineering approach to identify and implement best combination of systems and PF personnel to most effectively protect our security interests,"[2] and "We will use a risk management approach to identify that level of security protection that provides an acceptable and managed level of risk,"[3] the approach to staffing varies widely from site to site.

Without an NNSA policy that sets standardized criteria for validating PF operations, determining whether site PFs can adequately protect DOE SNM and critical assets will remain problematic. Each site has different methods and rationales for determining PF staffing, equipment, and training and for gauging whether protection is effective or adequate. The lack of a standardized, specific policy (formerly found in the superseded *Standards and Criteria Manual*) has led to this ad hoc approach.

Sites increase or decrease PF staffing with little documented analysis as to its effect on other projects or contingencies. For example, the shortage of personnel in the PF at one site—and thus its inability to protect multiple targets—has caused a shutdown of all test projects. That site's management greatly reduced the PF without considering the impact on other projects that needed safeguarding. At other sites, the PF staffing levels increased when an independent assessment by the Office of Independent Oversight and Performance Assurance (OA) and other audits showed serious flaws, and then decreased in years following successful audits and inspections. One site's PF staffing increased to meet contingency planning for one target, and then the site redirected the PF to address issues at other target locations, essentially leaving the first target as vulnerable as before.

No specific policy establishes methods sites can use to determine PF staffing levels through appropriate analysis or performance testing. Some determine staffing levels on the basis of JCATS analyses and others elect to use limited-scope performance tests. Very few sites conduct full-scale force-on-force exercises to capture an aggregate of pass and fail ratios with varying numbers of PF responders. All but one site declares that PF staffing levels are adequate for implementation of their protection strategies. This declaration may be true from the sites' perspective and demonstrated through their philosophy of analyses and testing, but determining its validity from the outside is difficult without clear policy for testing and validation.

Each site differs in how it uses response force times (RFTs) and pictures in time, and some don't use them at all. Some sites don't roll completed RFTs back into the VA analysis to determine their effectiveness in relation to adversary task time or incorporate them into force-on-force exercises or JCATS analyses. Without accurate RFT data, determining whether a site PF can respond in time with the appropriate numbers to interrupt or neutralize an adversary force is nearly impossible. No formal protocol describes how to test PF response time or how to roll test results back into the VA, which makes it difficult to determine whether appropriate analyses were completed to determine PF staffing levels.

---

[2] National Nuclear Security Administration, NNSA Safeguards and Security Strategic Plan, June 2003, p.1.
[3] See Note 2, p.2.

8.3.2 Clearance Process

The backlog in pending security clearances, because of the lengthy clearance approval process, has excessively increased NNSA overtime, affecting budgets and detracting from PF performance. NNSA has recognized this problem, and the strategic plan says it will "expand authorities and options for reducing time required to obtain security clearance and reinvestigation results."[4]

Excessive overtime budgets are still required for filling Q-cleared Personnel Security Assurance Program (PSAP) PF positions required by new DBT implementation plans and increased security condition levels.[5] New hires cannot fill positions until their clearances are granted, creating inordinate overtime demands for the already-cleared PF. As a result, sites must pay for the new hires who can't work the position and pay overtime to the cleared personnel who can. Excessive over-time leads to fatigue, burnout, and high turnover rates and can affect the PF's ability to conduct training and exercises because the officers are scheduled to work on days when training and exercises are often scheduled.

Facilities have a tremendous backlog of obtaining clearances for new hire PF personnel. Sites said that the Accelerated Access Authorization Program (AAAP) didn't work to expedite this effort because participants have to be too "squeaky-clean" to get through it.[6] Q clearances routinely require an average of more than a year, with another three months for PSAP approval.

8.3.3 Training and Qualifications

Adversary Pathways and Response Plans

Some site PFs do not receive adequate training in identified adversary pathways and their applicable response plans. DOE Manual 473.2-2 requires plans to address response to security incidents and adversary intrusion as described in the DBT policy.[7] In general, the existing response plans describe PF response activities, but usually contain little detail on the adversary attack methods and pathways identified and analyzed in the VA process. An effective PF should clearly understand adversary worst-case pathways and capabilities in addition to security incident response plans. Only two sites have trained PF personnel in VA probabilities and adversary worst-case pathways.

---

[4] See Note 2, p.6.

[5] In January 2004, DOE established the Human Reliability Program (HRP), which incorporates the important elements of the PSAP and Personnel Assurance Program (PAP) into one comprehensive program. Source: Federal Register, Volume 69, Number 129, July 2004. Available from http://edocket.access.gpo.gov/2004/04-15331.htm.

[6] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis,* Henry G. Chiles, Jr. et. Al., March 2004, p.2-9.

[7] U.S. Department of Energy, *Protective Forces Program Manual,* DOE Manual 473.2-2, June 2000.

Some sites do not require the PF to be familiar with or study and analyze response plans; these sites claim that response plan training takes place during force-on-force and tabletop exercises. This training approach is ineffective; at some sites, force-on-force exercise participation is voluntary, exercises are infrequent, and their relation to response plan review is questionable. No systems are in place to verify that appropriate PF personnel have participated in response plan training. Tracking individual participation in written response plan training is difficult at best. Officers on duty at any given time may not have read or been trained on these plans.

FIREARMS AND PHYSICAL FITNESS

Firearm and physical fitness qualifications are mandatory, but ongoing proficiency training between qualifications is optional at most sites. Not all sites re-quire SPOs to have firearm proficiency or physical fitness training between qualifications. Most allow officers to conduct voluntary training while on duty or make overtime hours available for them to schedule and conduct their own fire-arms proficiency and physical fitness training. At most sites, SPO IIIs take more advantage of this training than SPO IIs.

Physical fitness qualifications typically occur within a month of the officer's birthday, and firearm qualifications are semiannual, so many elect to only work out or practice several weeks before the test. This situation raises the question of whether the testing reflects the actual capability of the response force year-round or just individual capabilities at known test times—a question that becomes more critical as the PF ages.

RECAPTURE, RECOVERY, AND PURSUIT

Training and qualification are inadequate for recapture, recovery, and pursuit. In general, PF protection strategies focus on meeting only a portion of the worst-case DBT, denial of access. Although this strategy should be primary, sites need to have plans in place for denial of task, recapture, recovery, and pursuit contingencies to meet the full intent of the new DBT policy. Sites do not routinely test or validate preparation for these contingencies to demonstrate that they can perform missions should denial of access fail. Without these elements, sites are left with the potential for a single-point failure in their protection strategies.

FORCE-ON-FORCE EXERCISES

Force-on-force training at some NNSA sites lacks realism. It is difficult to con-duct realistic training exclusively at NNSA sites because the use of explosives, live fire weapons and, at some sites, even simulation type weapons are not al-lowed in the vicinity of storage facilities for safety reasons.

Site PFs are not conducting enough force-on-force exercises to maintain perish-able tactical skills. OA leadership has expressed a similar concern that the PF is stretched too thin across the complex and therefore not conducting enough force-on-force

testing, which leads to the loss of or reduction in perishable tactical skills and reduces overall efficiency. Force-on-force exercises are the closest replication of actual combat that can safely be used for training and evaluation of PFs. Sites should not use this valuable tool just to pass inspections or audits. If PFs do not frequently conduct these exercises and use the lessons learned to train their personnel, or if PFs substitute computer simulations or other training methods for exercises, their officers may not be tactically prepared to perform their missions.

8.3.4 VA and PF Coordination

At some sites, VA and PF personnel do not collaborate closely to ensure the accuracy and consistency of the VA and PF response plans. To ensure that response plans are effective and security systems are adequate for delay and detection, the VA and PF representatives must share information such as task times of adversaries, most likely pathways, and PF response times for interruption and neutralization of the adversaries. In the VA process, PF actual capabilities and accurate response times have to be captured in VA reports.

Some sites do not involve the PF adequately in the VA process. One facility does not include PF management in the initial review of VAs, and the VA planning group actually writes the PF response plans without PF participation—leaving the subject matter experts in tactics (the PF) without input to its response strategy. On the basis of lessons learned, one site now uses PF supervisors to write response plans, with the VA planning group, to avoid discrepancies.

8.3.5 Response Plan Effectiveness

Site response plans lack sufficient detail in several key areas. All sites except for one have active response plans in place, but most plans don't have detailed procedures for recapture, recovery, pursuit, communications, loss of communications, and chain of command. Some have conflicting information as to whether their target objectives are containment, denial of access, or denial of task. Sites that address these topics in response plans have either ineffective or contradictory planning information. For example, at one site, the VA group has a target objective listed as denial in its analysis, and the PF has the same target objective listed as containment in its response plans.

Local law enforcement and FBI cooperation with NNSA sites is severely deficient. Sites do not have memorandums of understanding/memorandums of agreement (MOUs/MOAs) with outside agencies to respond to potential contingencies. DOE Manual 473.2-2 states that sites that identify the need for outside agency support will establish formal MOUs/MOAs, annually update them with the off-site agency, and conduct annual force-on-force exercises.[8] Most sites have met with off-site federal and local law enforcement agencies (LLEAs) but coordination has generally been limited to discourses and table-top exercises. Other unresolved issues involving coordination with LLEAs include the following:

- Overall tactical command responsibility
- Different use-of-force policies
- Appropriate maximum speed during a pursuit
- Conflicts among internal documents concerning pursuit tactics and coordination with LLEAs.

In general, sites that deputized selected PF staff into the LLEA or established a federal officer program within their PF had more success in bringing the LLEA and site PF personnel together on these issues.

8.3.6 Target Folders

Only half of the sites visited have some form of target folders in place; none of the sites completely follow the approved, enhanced guidance of the 1998 McCallum memorandum.[9] This memorandum—developed and agreed upon by DOE and FBI headquarters—gives specific guidance as to what the DOE target folders encompass. The remaining sites do not have target folders in place, or they are not sufficient for planning purposes. Only two sites have target folders sufficient for tactical planning for basic response and, more important, recapture and recovery (R&R).

Sites develop target folders to assist the PF and outside law enforcement agencies in conducting interagency-compatible tactical operations. However, sites are un-sure of what the target folder includes and the approved format. DOE Order 473.2-2 directs sites to follow OSS director guidance, which outlines the required information and approved format. In addition, during semiannual SRT quality panel meetings, the DOE Office of Security (SO) encouraged site representatives on the panel to use the director guidance.

---

[8] See Note 7.

[9] U.S. Department of Energy, memorandum from Edward McCallum, Director, Office of Safeguards and Security, to DOE director distribution, subject: *Enhanced Target Folder Development and Use,* June 4, 1998. DOE Manual 473.2-2 (see Note12) directs that site target folders use the format and content approved by the Office of Safeguards and Security (OSS) Director. The memorandum from Director McCallum describes the current approved format and content.

8.3.7 Chemical and Biological Weapon Defense

The NNSA-wide response to the chemical and biological weapons (CBW) threat lacks uniformity. All sites have respirators and limited personal protective equipment (PPE) clothing. [REDACTED]

8.3.8 Central Alarm Station Alarm Rates

Some sites' central alarm station (CAS) false and nuisance alarm rates are excessive or not tracked. One site's false or nuisance alarm rates are in the thousands per month. In effect, portions of the protective system are not operational because the CAS operator has to access (turn off) or ignore the alarms as a nuisance be-cause there are too many to assess and respond to. This increases the risk to the protected area, and this risk is not accurately reflected in the site's VA. For example, if the site's VA takes a large amount of credit for certain properly working protection elements, then it should also accurately reflect degraded operations. Another site's alarm administrator, who had no false or nuisance alarm data, said the site system is antiquated.

In general, the PF is not properly trained in recording alarms; for example, the difference between nuisance (environmental or animal caused) and false (un-known and needing assessment) alarms is frequently not made. Understanding the difference is critical to documentation and evaluation of the system's effective-ness.

8.3.9 Recapture, Recovery, and Pursuit

RECAPTURE AND RECOVERY (R&R)

Site R&R contingency plans are nonexistent or inadequate.[10] The sites explain that they focus on a denial-of-access strategy. Denial of access is the primary mission of NNSA sites, and resources and efforts should be dedicated to developing robust denial strategies. However, some sites' reliance on the viability of their denial strategies has precluded them from adequate planning, training, and procurement of appropriate tools for R&R should denial fail. Some sites' R&R plans incorporate a

[10] This does not include plans of the Nuclear Emergency Search Team, which we did not review.

denial-of-access strategy that inappropriately assumes they will never lose control of the facility. If adversaries gain access to a facility or leave with material, R&R programs are critical. Furthermore, the new DBT policy established site responsibility for instituting an R&R program.[11]

Site safeguards and security plans (SSSPs) and some facility response plans ad-dress R&R programs and plans, but they vary widely, and some do not fulfill the need for a timely, effective, and viable R&R capability or meet the intent of DOE Manual 473.2-2.[12] Some approaches include R&R response activities and requirements (spread throughout different response documents) but do not identify one specific response plan for R&R of an SNM storage facility or material in un-authorized control.

Other R&R approaches include tactical options that are rudimentary, very high risk, and not tactically viable. For example, the mechanical and electronic entry techniques used at some sites have not been performance tested or fully evaluated for their effectiveness, and, during iterative site analysis (ISA) processes or OA inspections, some of these techniques have failed testing. DOE Manual 473.2-2 states that when mechanical entry alone will not meet required response times, the site or facility must develop an explosive tactical entry capability.[13] [REDACTED]

[REDACTED]

Although the elements of response plan training and testing are critical to effective R&R programs, very few sites have conducted actual training or testing, and those that have use tabletop activities or walk-through drills.

Adversary capabilities continue to increase, but NNSA threat planning lacks dedicated offensive response teams for each site to meet these threats. The manpower-intensive denial-of-access strategy requires numerous PF personnel dedicated to a material access area (MAA) in a repel-type posture. Sites say that the resources committed to this effort prevent them from assigning an offensive force as a dedicated, ready, and equipped element for R&R response activities.

[11] U.S. Department of Energy, memorandum from Robert Card, Under Secretary, to Field Operation Office Directors, subject: *Design Basis Threat,* May 20, 2003.
[12] See Note 7.
[13] See Note 7.

The DOE system has an offensive PF program (SPO IIIs),[14] but most sites utilize SPO IIIs in a defensive position, often separating them to operate individually or with SPO IIs not trained in team tactics. This use defeats the purpose of a highly trained offensive team that can rapidly and aggressively respond to R&R options and other adversary attacks and constitutes nothing more than using SPO IIIs as highly trained SPO IIs.

PURSUIT

Sites do not have sufficient planning, equipment, and training to conduct pursuit operations. Pursuit capability is a critical component of effective R&R. Most sites have not conducted recovery or pursuit training or exercises beyond the protected area of a facility, even on-site. [REDACTED]

Pursuit guidelines allow PF personnel to use vehicle immobilization techniques and tire deflation systems, and fire at and from moving vehicles (all of which fall under deadly force). To maintain pursuit capability, sites need to provide emergency vehicle operation course (EVOC) training, a perishable skill that requires refreshing and practice. However, most sites do not provide this training due to resource limitations.

8.4 RECOMMENDATIONS

1. Establish policy to ensure that protective force staffing is based on an ac-curate VA. Include specific guidance to help sites prepare plans for PF staffing, equipment, and training in a defendable and consistent manner to eliminate the wide variation in site to site interpretation.

2. Increase clearance investigation personnel staffing to help reduce the security clearance backlog.

3. Adopt the recommendations of the Security Affairs Support Association (SASA) "to improve and streamline the current processes for granting new security clearances and reinstating existing accesses."[15]

4. Direct sites to train or brief the PF on VAs, including worst-case adversary pathways, task times, and adversary attributes.

---

[14] In addition to SPO II training, SPO IIIs take a 3-week course in room-clearing tactics, receive limited tactical operation training, and have slightly higher physical fitness and firearms standards. However, these qualifications alone do not completely fulfill R&R mission needs.

[15] Letter, from Kenneth A. Minihan, President and Chairman of the Board, SASA, to directors of various agencies, February 13, 2004. Available from www.greaterla.isac.com/docs/sasaltrtodci.doc.

5. Have sites establish formal training to ensure that all PF personnel have current knowledge of response plans and strategies.

6. Consider establishing requirements for more frequent weapons and fitness training, rather than making it optional between qualifications.

7. Consider conducting random testing of the PF throughout the year in both firearms and physical fitness. This testing will encourage officers to maintain weapons skills and physical fitness levels year-round and will give management a more realistic picture of the overall PF's capabilities.

8. As recommended by the ETE Review, NNSA, in partnership with DoD, should establish a national training center for protective forces. The center should provide for realistic, force-on-force training against a well-trained, well-equipped adversary that simulates the DBT. The facility should be flexible enough to allow simulation of representative storage and transportation configurations. Training should be scheduled to allow all protective forces to participate at least once every two years.[16]

9. Ensure that sites are required to routinely and frequently conduct force-on-force exercises to evaluate and train in the tactical skills needed for com-bat operations.

10. Direct the standardized use of PF subject matter experts in the development of VAs and PF response plans to ensure the cooperation and integration of personnel responsible for effective protection strategies. Promote greater collaboration between site VA teams and PFs to develop VAs and response plans.

11. Direct site offices to ensure that target folders meeting DOE guidance are in place to tactically plan an R&R operation and support other strategies identified in site incident response plans. Consider giving the site office, PF, and local law enforcement or FBI (the entities with a vested interest, should the need for target folders arise) final approval of target folders.

12. Consider consolidating the various memos, guides, and policies concerning target folders into a single policy document.

13. Establish, with appropriate urgency, a CBW defense policy. It should identify specific criteria for implementation of specific levels of CBW equipment, including a minimal level of PPE, training, and detection. Develop a baseline threat for CBW, detailed enough to assist sites in identifying their program

[16] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Indpenedent Assessment of the U.S. Nuclear Command and Control Systems (U),* Final Report, April 2002 (Top Secret)

needs and providing a good rationale for SSSP documentation as required by DOE order. The identified criteria and threat will provide sites and headquarters a tool to plan for appropriate funding and implementation, including development of an exercise and testing pro-gram for effective evaluation.

14. Direct site offices to regularly check the false or nuisance alarm rates from the CAS and compare them with the credit taken in the VAs to ensure the analysis accurately reflects field conditions. Establish a method to properly record and document the false or nuisance alarm rate and ensure proper training for CAS PF personnel. Install modern computer alarm equipment that has an automated alarm tracking system to replace antiquated systems.

15. Ensure sites establish viable, effective R&R plans, which include exploring the need to retake a facility and the most current tactical methods (mechanical and explosive breaching) available. Sites should analyze and document the practicability of an explosive breaching strategy for their specific storage facility. [REDACTED]

16. Direct sites to establish testing and evaluation of R&R contingency plans, including evaluation criteria, to determine the effectiveness of the pro-gram. Require each site to maintain a dedicated offensive force—trained, equipped, and responsible for R&R missions. Consider creating a training program that includes offensive team tactics and tactical entry techniques for hardened targets in line with current R&R needs. Ensure sites have the ability to train and equip their PFs with the most current methods of R&R and pursuit, including hands-on training with equipment, coordination, and exercises with outside agencies.

17. Urgently establish and periodically revalidate MOAs with the FBI and local law enforcement agencies (LLEAs) for each applicable NNSA site. Improve FBI and local law enforcement cooperation with NNSA sites to include development of recapture/recovery plans for appropriate sites and actual exercises (i.e. not just table-top) of plans in recapture/recovery scenarios. Consider encouraging sites to deputize some site PF personnel into surrounding LLEAs or establishing a federal officer program.

18. Establish policy detailed enough to enable sites to prepare response plans covering R&R, pursuit, communications, loss of communications, and chain of command. Direct sites to prepare realistic pursuit plans that detail chase parameters.

19. Establish policy that directs sites to have a dedicated offensive element—separate from the denial-of-access contingent—that can implement R&R and other offensive missions like pursuit, ambush, and counter-sniper actions.

Section 9
Security Incidents and Inquiries

9.1 BACKGROUND

The reporting, investigation, monitoring, and analysis of security incidents within NNSA are vital to the overall protection of NNSA assets. A successful, robust program includes timely identification and recognition of incidents, proper categorization by consequence and seriousness, timely notification of appropriate management, full investigation, adequate corrective action, and dissemination of lessons learned to prevent recurrence. DOE recently replaced DOE Notice 471.3 and issued DOE Order 471.4, *Incidents of Security Concern*, to set forth program requirements.[1]

9.2 SUMMARY

The reporting, investigation, monitoring, and analysis of security incidents within NNSA are hindered by inconsistent practices, redundant reporting, and inadequate reviews. More formal and disciplined processes are needed to ensure the underlying causes of incidents are identified and addressed, appropriate corrective action is effectively implemented, and lessons learned are disseminated within NNSA to mitigate against recurrence.

9.3 OBSERVATIONS

9.3.1 Inconsistent Incident Categorization

DOE Order 471.4 describes the categorization of incidents of security concern as follows:

> Incidents of security concern are categorized in accordance with their potential to cause serious damage or place safeguards and security interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of

[1] U.S. Department of Energy, *Incidents of Security Concern,* DOE Order 471.4, March 2004.

physical security, protective forces, information security, personnel security, and nuclear material control and accountability[2].

Sites inconsistently categorize incidents using the IMI tables in DOE Order 471.4 because interpretations vary widely from site to site. For example, some incidents that should have been categorized and reported as IMI-3 or -4 were categorized as not reportable. Other incidents that should have been categorized as IMI-2 or -3 were categorized as IMI-4, which allows monthly compilation reporting instead of reporting to headquarters within 8 hours of categorization.

The following are examples of inconsistent site categorization of incidents of security concern using the DOE Order 471.4 IMI tables:

- At some sites, instances of personal cell phones found inside limited areas were categorized as IMI-3, and at another site, as IMI-4.

- At one site, an incident where a camera and cell phones were found inside a sensitive compartmentalized information facility (SCIF) was categorized as IMI-4; at other sites, this incident would have been categorized as IMI-2.

- At one site, some instances involving classified information on unclassified computers were categorized as non-incidents or IMI-4; at other sites, they were categorized as IMI-1, -2, or -3, as appropriate for the level of classified information and duration exposed.

- At another site, an unsecured alarm point was categorized as a non-incident. At the other sites visited, this incident would be categorized as IMI-4.

- At one site, an incident involving a Category IB of U^{235} left outside a vault overnight was categorized as the lowest IMI-4. This incident should have been categorized as IMI-2 and reported to the Office of Security (SO) within 8 hours of categorization. Because it was categorized IMI-4, the only notification SO received was an end-of-month compilation report of IMI-4 incidents at the site. Personnel did not inform contractor security management, site office security management, SO, or NNSA of the incident as required.

- Some sites are incorrectly interpreting "more than 8 hours" (under IMI-4 type 13) to mean that if an unclassified PC or network on which the classified information resides can be pulled offline, secured, or sanitized within 8 hours of discovery, the incident can be categorized as IMI-4 or a non-incident—no matter how long the classified information resided (and was vulnerable) on the unclassified PC or network.

[2] See Note 1, p. I-2.

The current incident reporting process allows (and somewhat encourages) the recategorization of incidents to a lower consequence when sites determine that no compromise of classified information occurred. Some sites downgrade the incident category after determining that no compromise or potential compromise of classified information occurred, and others do not. This inconsistency hinders efforts to obtain and track meaningful metrics that reflect the type and seriousness of incidents that have occurred. The recategorization and submittal of a new DOE Form 471.1 to change the incident from the initial, more serious category to a lesser one obscures the potential seriousness of the initial incident.[3] This practice gives DOE/NNSA senior managers a false sense of security; when incidents are recategorized, DOE/NNSA management is precluded from evaluating the potential gravity of the initial incidents or number of near misses, which could be pre-cursors of a more serious security problem.

9.3.2 Redundant Reporting Systems

Incident reporting systems are redundant. DOE requires the reporting of incidents under the DOE Office of Security (SO) purview through the Incidents of Security Concern (IOSC) reporting process to headquarters. Additionally, security-related safety incidents are required to be reported through the Occurrence Reporting Processing System (ORPS). These different reporting systems are not integrated, so one incident is sometimes reported through more than one channel or system to headquarters. This redundant reporting can lead to confusion. Finally, DOE Notice 205.4 requires the reporting of cyber incidents—such as unauthorized access, malicious code, denial of service, and scans and probes—through cyber channels to the Computer Incident Advisory Capability (CIAC).[4]

9.3.3 Inadequate Incident Inquiries and Report Review

Some site offices, NNSA headquarters, and the DOE Office of Security (SO) do not sufficiently review final inquiry reports for adequacy, completeness, and thoroughness of inquiry. The panel noted a number of inadequate IMI-1 and -2 reports at one particular site and a lack of thoroughness in investigating certain cyber incidents at another.

At one site, the cyber organization does not give incidents of security concern the same priority as the inquiry team does, so its support is not as forthcoming or complete as it should be. The cyber organization reportedly does not want to generate any classified information, so it does not provide adequate reports to the inquiry officials. Review of a number of inquiry reports found a failure to fully investigate cyber incidents, for example, determining whether further dissemination of the classified information went beyond the initial distribution or whether uncleared or non–U.S. citizens were in proximity to computers containing classified information.

---

[3] U.S. Department of Energy, *Security Incident Notification Report*, Form 471.1.

[4] U.S. Department of Energy, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents,* DOE Notice 205.4, March 2002.

The adequacy of transient electromagnetic pulse surveillance technology (TEMPEST) experience and knowledge for those involved in conducting official inquiries is lacking. At most sites visited, the distance from unauthorized cellular telephones to classified processing equipment is not considered in the investigation and evaluation of an incident.

One site generates brief, inadequate IMI-1 and -2 final inquiry reports and uses Form 5639.3, "Report of Security Incident/Infraction," almost exclusively for all incidents (IMI-1 through -4). DOE Order 471.4,[5] DOE Notice 471.3,[6] and Secretary Memorandum, June 14, 2002, require full, [7]final reports for IMI-1 and -2 incidents. Form 5639.3 is only to be used for IMI-3 and -4 incidents.[8] The continuation of this practice for some time reinforces the observation that the site office, NNSA, and DOE headquarters do not appropriately review final inquiry reports. An SO representative stated that his office has not reviewed final inquiry reports since about 2001 when his office was taken out of the oversight role; how-ever, NNSA has not, until recently, exercised their responsibility for final incident report review. NNSA recently assigned an employee as its point of contact for incidents of security concern. This employee is awaiting classified workspace but stated that part of her new responsibilities will be to review all final NNSA inquiry reports and return inadequate reports to the originator.

The process for incident closure does not sufficiently involve final report review for adequacy and promulgation of lessons learned. Sites submit initial incident reports to the DOE Operations Center for appropriate distribution, and final incident reports are sent to the Office of Security (SO). Although copies of the initial and final reports are provided to NNSA, closeout is conducted by SO—which does not have direct, day-to-day oversight responsibilities for NNSA sites. Incidents are inappropriately closed out upon receipt of a final report at SO, rather than upon NNSA review of the final report for adequacy of corrective action and dissemination of lessons learned.

9.3.4 Inadequate Tracking and Communication

At most sites, a formalized and disciplined site-level process for tracking security incident corrective actions is lacking. As a consequence, determination of whether appropriate corrective actions have been institutionalized is difficult. Most sites reported that line management is responsible for tracking and implementing corrective actions identified by an inquiry into an incident of security concern. However, most sites do not have a formalized, disciplined process for tracking and verifying that identified corrective actions were properly implemented. Site senior supervisory awareness and oversight of the status and completion of corrective actions is needed.

One site does have a good manual method of tracking the corrective actions at the

---

[5] See Note 1, p. 1-8

[6] U.S. Department of Energy, *Reporting Incidents of Security Concern,* DOE Notice 471.3, April 2001.

[7] U.S. Department of Energy, memorandum from Spencer Abraham, Secretary of Energy, to Lead Program Secretarial Officers, subject: *Reporting Incidents of Security Concern,* June 14, 2002.

[8] See Note 1. p. 1-9.

inquiry official and specific incident line management level. However, without a site-level tracking process, timely completion and sharing of incidents and actions—to preclude similar incidents at the same site—is difficult.

DOE/NNSA has no dedicated, formalized program for reviewing incidents, analyzing root causes, verifying adequacy of corrective actions, and disseminating lessons learned across DOE/NNSA to promote awareness and minimize recurrence. Although DOE/NNSA has a variety of means for disseminating information, the ad hoc process for disseminating security incident lessons learned is not timely, complete, or effective.

The Chiles report found the following:

> Incident reviews, root cause analyses, corrective action plans, and corrective action tracking are common elements of each site's security pro-gram. Specific issues and incidents vary among the sites, but a number of common areas have bearing throughout.
>
> The complexity of NNSA activities, level of staffing, and continuously evolving security challenges underscore the importance of both informal and formal mechanisms for the timely communication of issues and application of lessons-learned within and across the NNSA sites. This practice is similar to those for sharing lessons-learned from safety evaluations and incidents.
>
> The coordination and sharing of security lessons-learned is an important responsibility for NNSA. Dissemination of this information helps improve security performance within the NNSA complex, provides a highly beneficial training and development tool for the federal security staff, and helps strengthen professional relationships within the security work-force. An effective synthesis of lessons-learned from internal security re-views and recurring external inspections of NNSA and other DOE sites serves not only to improve security performance at the evaluated site, but also helps to identify site and complex-wide trends and leading indicators that can be communicated throughout the complex.
>
> NNSA has a variety of methods for disseminating current issues, best practices, and lessons-learned: participation in quality panels, periodic S&S directors conferences, monthly conference calls involving S&S directors, lessons-learned database systems, and an occasional newsletter or special e-mail. NNSI also conveys current issues. Nevertheless, the current processes have limitations. For example, lessons-learned are not published regularly. Only 9 percent of our survey respondents strongly

agree that the lessons-learned process is timely and effective, and fully 30 percent did not consider it so.[9]

9.3.5 Inadequate Security Incident Metrics

Security incident metrics provided quarterly to senior DOE and NNSA headquarters leadership are inadequate to monitor and assess security program performance. They do not reflect the true nature of the incidents and near misses occurring across the complex. Examples include the following:

- The metrics inordinately focus on comparing sites' incident closures as measures of success rather than on analysis of underlying causes (such as procedures, training, materiel, and personnel) and occurrence trends. One headquarter's metric compares open to closed incidents at each individual site. If a site has a number of incidents open compared with other sites, it reflects negatively in the metrics. In effect, sites are positively recognized for incident closure rather than for thoroughness of inquiry and adequacy of corrective action. Additionally, this measure does not accurately reflect whether sites close inquiries within 60 working days (as required by order for IMI-1 and–2 incidents).

- One metric, for information security incidents, weights them according to the classification level or type of the information involved, regardless of the IMI number of the incident and whether the information was compromised or not. In effect, incidents involving top secret, special access pro-gram (SAP), or sensitive compartmentalized information (SCI) material where no compromise occurred are routinely graded more negatively than a compromise of secret national security information (NSI) material.

- IMI-4 incidents are not included in the quarterly metrics because sites only report IMI-4 incidents monthly as a compilation and do not include information on the level or type classified information involved. When incidents are recategorized down to IMI-4 (after determination that no compromise occurred), they are not factored into the metric. As a result, senior leadership is unaware of the nature and frequency of potentially serious incidents determined to be near misses.

- Cyber security incidents are not fully integrated in the security incident metrics because of a lack of collaboration between SO and the DOE CIO and their separate incident reporting systems.

[9] NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: In Independent Analysis,* Henry G. Chiles Jr. et al., March 2004, pp.2-10 and 2-11

9.3.6 Inconsistent Infraction Administration

NNSA guidance on implementation and application of the infraction program is lacking. This omission results in widely varying local interpretations of criteria for charging individuals with security infractions. Some sites have different levels of security infractions and occurrences, warnings, or near misses. An employee at one site may receive an infraction for an action that would incur only an occurrence, warning, or near miss at another site.

There are no clear standards for what constitutes in an infraction, and thus there are consistencies across the complex. For example, many sites issue infractions to employees who introduce personal cell phones into security areas. In contrast, one site did not issue an infraction when an employee brought a personal cell phone into a sensitive compartmentalized information facility (SCIF). The same site sometimes issued infractions when the cell phones were introduced into limited areas. Another site office did not issue infractions to a number of employees who put classified information on unclassified PCs. Some sites that have more than one level of infractions, warnings, occurrences, or near misses do not provide re-ports of certain levels to the personnel security office as required for derogatory information. Because infractions are considered derogatory information in clearance reviews, administration of infractions needs to be more standardized.

9.3.7 Inadequate Inquiry Resources

NNSA has a shortage of experienced and qualified inquiry officials across the complex (at all sites), and some of the security incident organizations lack administrative support. The increase in incidents has outpaced staffing levels to report and conduct the inquiries. The shortage prevents timely investigation, reporting, and closure of incidents. It can also rush completion of an inquiry, impede a thorough investigation, and hinder the sites' ability to proactively reduce incidents. Some sites have difficulty completing the inquiry and reporting closure within 60 working days as required.

Organizations outside of the inquiry teams sometimes fail to provide timely and effective support to the team or official in incident resolution. For example, at one site, Human Resources does not review draft inquiry reports in a responsive manner to determine disciplinary action, and, at some other sites, line management does not conduct or support timely causal analysis or provide timely corrective action plans. One site had a cyber incident involving Sigma 15 weapon data on hold because no one had the access to forensically examine a hard drive at the site, and the site had not obtained resources from off-site to do so.

None of the contractor inquiry officials visited has been issued the DOE Basic Security Credential. Though infrequently needed, the Basic Security Credential allows inquiry officials to properly identify themselves on the few occasions when their authority is questioned. The DOE Basic Security Credential is avail-able for issuance and has been issued to contractor inquiry officials at some non-NNSA sites. One site office requested Basic Security Credentials for its contractor inquiry

officials from headquarters over a year ago and still had not received them at the time of our visit.

Each of the inquiry teams visited was at least four levels removed from the site director. The site director has responsibility for supporting and ensuring full investigation and reporting of incidents and complete, timely corrective actions. Excessive levels of management between the inquiry team and the site director can reduce the importance of the function in the eyes of site management and employees, and reduce site director awareness of incidents occurring at the site.

Many of the people assigned and available to conduct inquiries at the sites do not possess the access needed to perform inquiries into all of the potential incidents that could occur at the site. Each site director should have the capability to enlist people (external to the program that caused the incident) with appropriate accesses to quickly respond to and fully investigate any security incident that may occur at that site. Once an incident occurs, it may be too late to grant access, which delays the response to the incident, preventing an adequate inquiry.

Some sites allow the special security officer (SSO) for a SCIF or the SAP security manager to conduct inquiries into incidents in their own programs, which are among the most sensitive. This is not appropriate and many times is a clear conflict of interest. When this type of incident occurs, a cleared and appropriately trained individual—trusted by management and independent of the affected SCI or SAP—must be assigned to conduct a full inquiry. This person does not have to be an inquiry official from the IOSC team, but should be inquiry-trained and external to the affected program.

9.4 RECOMMENDATIONS

1. Provide timely interpretive guidance and training to ensure the IMI tables are consistently applied.[10] Ensure guidance on urgency of incident report submissions is clear.

2. Ensure individuals notify site offices of all incidents as they are categorized to provide timely oversight of incident categorization and eliminate or reduce the potential for incident miscategorization.

3. Eliminate the policy and practice of incident recategorization on the basis of a determination that no compromise occurred. The final inquiry report contains the information needed to indicate whether a compromise did or did not occur.

4. Consolidate reporting systems into a single system to eliminate redundant reporting, standardize reporting elements, and facilitate adoption of a common incident database. Use distribution controls at headquarters, rather than separate report formats, to ensure different categories of incidents are routed to the

[10] See Note 1, pp. 1-3 – 1-7.

appropriate people.

5. Establish a more rigorous process within DOE/NNSA headquarters to thoroughly review initial incident reports; monitor the inquiry progress; review final reports for adequacy of the inquiry, corrective actions, and analysis of underlying causes; and keep senior DOE/NNSA leadership appropriately advised.

6. Close incidents only after DOE/NNSA headquarters has reviewed and approved the final incident report, rather than upon receipt at headquarters.

7. Educate all organizations regarding the priority of incidents of security concern and importance of responsiveness and cooperation in the inquiry process. Encourage site managers and directors to educate their employees and management on the importance of timely support to inquiry teams.

8. Establish a more formal and disciplined process at sites to track security incident corrective actions to completion. Consider requiring site management to include findings and corrective action plans in a site-level corrective action tracking process involving senior line management to ensure corrective actions are adequate and complete. Ensure reviews are con-ducted to execute continuous improvement. Have all site offices randomly review corrective actions for completion during surveys, and have the Office of Independent Oversight and Performance Assurance (OA) review a sample during performance inspections.

9. As also recommended by the Chiles report, establish a dedicated and more effective formalized process within NNSA headquarters to disseminate incident lessons learned to the NNSA community.[11] Consider publishing a quarterly lessons-learned message for all DOE/NNSA sites, with procedures for ad hoc promulgation of urgent lessons learned.

10. Develop more meaningful security metrics that accurately measure the nature, frequency, and significance of incidents; the underlying root causes; and the timeliness of reporting, investigation, and corrective action development. Periodically provide these metrics to senior headquarters and site leadership, as well as appropriate security officials, to promote greater awareness of security performance and concerns.

11. Review the infraction programs and provide guidance for standardization to enable consistent application across DOE/NNSA sites. NNSA site offices should review the infraction programs at their facilities to ensure the infractions are administered consistently for federal employees and contractors.

12. Assess the adequacy of IOSC staff levels complex-wide to ensure they have sufficient people and expertise to conduct and report adequate, complete inquiries.

13. Issue the DOE Basic Security Credential to all DOE/NNSA-approved inquiry

[11] See Note 9.

officials.

14. Consider temporarily assigning the inquiry official as a direct report to site management during the course of an investigation to effectively reduce the number of management levels between the incident inquiry team and the contractor site director.

15. Ensure procedures are in place to avoid the perception that an individual conducting an inquiry has a conflict of interest or bias in the possible out-come of the inquiry. Discontinue the practice of having SSOs and SAP security managers conduct inquiries into incidents involving their own programs.

Section 10
Design Basis Threat Implementation

10.1 BACKGROUND

The events of September 11, 2001 dramatically illustrated that the accepted tenets of the then-existing postulated threat to nuclear weapons and material were no longer valid. As a consequence a new postulated threat was produced by the intelligence community in January 2003 and became the new foundation for the DOE's Design Basis Threat (DBT). The new DBT was promulgated by DOE in May 2003.

Countering a new, potentially larger, and more sophisticated threat to nuclear weapons and material has required senior leadership within NNSA to reevaluate existing security and protective forces and upgrade them to meet identified vulnerabilities. In fall 2003, NNSA took steps to begin implementing the new DBT: requesting initial cost inputs and draft implementation plans from the sites and hosting meetings at headquarters to get additional input and review the plans. Several interrelated issues needed to be resolved to get viable implementation plans and accurate associated costs; but, to meet budget-cycle requirements, NNSA and DOE pressed forward to obtain whatever time and cost estimates they could for DBT implementation. The stated goal is full implementation by the end of FY06.

In April 2004, the General Accounting Office (GAO) published a report which questioned whether this goal could be met for all sites.[1] Specifically, it questioned the time it took DOE to formulate the new DBT; its decision to use lesser threats than the Defense Intelligence Agency postulated threat; possible weaknesses in the criteria for protecting against new terrorist threats, such as chemical, biological, and radiological sabotage; and DOE's slowness in issuing guidance, preparing implementation plans, and developing adequate budgets.

[1] U.S. General Accounting Office, *DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat,* GAO-04-623, April 2004. Available from http://www.gao.gov/new/items/d04623.pdf.

10.2 SUMMARY

There has been insufficient collaboration between DOE and DoD and among NNSA sites in translating the intelligence community's postulated threat into security requirements. As a result, NNSA security standards differ:

- from those of DoD nuclear weapons facilities, because DOE/NNSA has taken a different approach to dealing with the postulated threat than that of DoD, and
- from site to site, because sites have interpreted terms such as insider threat, mission-critical facilities, escorting policies, and improvised nuclear devices (INDs) differently.

Determining whether NNSA will meet DBT implementation objectives by FY06 is difficult: the process for managing the program and funding requirements largely depends on the sites' interpretations of DBT requirements.

10.3 OBSERVATIONS

10.3.1 Insufficient Collaboration and Guidance

DOE/NNSA has taken a rational approach to converting the intelligence community's postulated threat into a risk-based DBT. The only substantive criticism is that the approach was taken in isolation, without any apparent collaboration with DoD, despite recommendations for greater coordination between the two departments.[2] On its own, DoD has belatedly adopted a dramatically different approach, not fully consistent with DOE's. The result of the profoundly different approaches is that the same nuclear weapons under nearly identical conditions are not protected under the same or equivalent security standards. From a national security perspective, the lack of security equivalency is inexplicable and unwarranted.

DOE/NNSA has not provided sufficient, clear guidance on DBT implementation to ensure consistent interpretation department-wide. DOE/NNSA headquarters and the sites have not sufficiently collaborated to develop a shared appreciation of the measures required to meet the new DBT. Examples of this lack of guidance and collaboration include the following:

- NNSA has not provided sufficient guidance to the sites for defining mission-critical facilities, which require a higher level of protection. Without this guidance, the sites are trying to determine whether they have mission-critical facilities with protection requirements as specified in the new DBT

although the sites can clearly identify the activities critical to their missions, NNSA headquarters should clearly identify the missions that are critical to national security. The inconsistent interpretation of mission-critical facilities is likely to greatly increase the cost of facility protection because the sites will err on the side of caution, unnecessarily requiring the deployment of more security resources than may be actually needed.

- As identified in a GAO report,[3] the criteria established for protection of facilities may not be sufficient. For example, the "industry standards" that sites are required to implement to protect against chemical sabotage have yet to be developed. Similarly, the criteria for protection against radiological sabotage may be inadequate to prevent radiological dispersal over wide areas (see Section 12).
- The guidance for sites with improvised nuclear device (IND) concerns is still evolving,[4] and it could eventually result in more costly than anticipated protection strategies. To date, sites have implemented inconsistent solutions for meeting this requirement.
- DOE policy does not clearly define the new DBT insider threats, particularly with respect to escorting policies; as a result various sites have interpreted the term differently. Policies regarding personnel allowed within protected areas, escorted or unescorted, differ from site to site. Some re-port certain acts as violations, and others do not; some apply a less rigorous policy than others. Some sites are interpreting the policy in their own interest, to require less work to be performed or to redefine the problem in a way that minimizes the need for protection strategies. For example, some sites have interpreted the DBT policy on escorting of non-Personnel Assurance Program (PAP)—now Human Reliability Program (HRP)—employees within the material access area (MAA) to mean escorted employees are exempt from being insider threats.

10.3.2 Inconsistent Site to Site DBT Implementation

The site to site implementation approach to DBT implementation has resulted in inconsistent interpretation of guidance across the complex:

- Some sites have conservatively interpreted the new DBT requirements and requested significant additional resources, while other sites (recognizing the existing tension between the new DBT requirements and available re-sources) have based their DBT implementation requirements on anticipated security budget levels.

---

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U), Final Report, April 2002 (Top Secret).
[3] See Note 1.

- As discussed earlier, the weaknesses and uncertainties noted in the individual site vulnerability assessment (VA) and site safeguards and security plan (SSSP) processes create significant uncertainties in the validity of the assessments which underpin the new DBT implementation plans.

- One submitted SSSP acknowledges that a certain threat exists per the DBT, but then analytically excludes that threat and assumes the risk for that particular adversary capability. This practice—basing upgrades on an assessment that excludes specific DBT attributes—may prove costly if the site is ultimately required to implement all attributes of the DBT.

As discussed in Section 12, the lack of an enterprise-wide approach to special nuclear material (SNM) consolidation has significant implications for DBT implementation. The antiquated, dispersed facilities in which some SNM is stored require more security manpower and resources than more modern structures on a reduced footprint. Accordingly, the DBT implementation scope and costs are likely to be larger for NNSA's older facilities located within a larger protection footprint.

Finally, the site to site implementation approach complicates DOE/NNSA's ability to prioritize resource requirements to address the most critical vulnerabilities identified as part of the new DBT implementation. NNSA relies on individual site assessments and periodic independent OA performance assessments to validate DBT implementation, rather than directly performing its own assessments.

10.3.3 DBT Implementation Resources

It is difficult to assess whether there are adequate resources, programmed or planned, to meet the new DBT implementation deadline of FY06 because of many of the factors cited above—uncertainties associated with the sites' assessment methodologies, inconsistencies in the sites' interpretation of DBT policy requirements, potential funding impacts of SNM consolidation, and evolution of guidance on INDs, as well as the lack of a robust resource-requirements validation process as described in Section 13.

10.4 RECOMMENDATIONS

1. Collaborate with DoD to reconcile the differences between approaches to the postulated threat, and establish equivalent, if not identical, approaches to address it, such that protection standards for nuclear weapons and material are fully consistent for essentially equivalent conditions. The Nuclear Weapons Council [REDACTED] may be the appropriate forum for such collaboration.
2. Establish a collaborative process to achieve complex-wide consistency and standardization in DBT policy interpretation and implementation. DOE/NNSA must provide clear guidance on the definition of mission-critical facilities, protection requirements for INDs, criteria for protection against chemical and

[4] [REDACTED]An IND is a device designed or constructed outside an official government agency which has, appears to have, or is claimed to have the capability to produce a nuclear explosive.

radiological sabotage, and requirements associated with protection against the insider threat.

3. Adopt a comprehensive and integrated department-wide approach to DBT implementation by consolidating individual site DBT implementation plans into an NNSA master DBT implementation plan. As part of this consolidation, incorporate initiatives that have the potential to reduce re-source requirements, such as SNM consolidation and infrastructure recapitalization. This action will facilitate gap analysis, result in improved prioritization and utilization of scare resources, and assist in developing a realistic budget. The master DBT implementation plan should include the following:

   - Improved justification and validation of DBT implementation requirements based on more consistent and robust VAs, SSSPs, and performance-testing processes (see Section 7.)

   - Centralized responsibilities and accountability for plan validation and implementation within NNSA headquarters (see Section 13.)

4. As recommended in Section 13, in the near term, consider establishing an independent panel to validate the adequacy of funding to implement both the new.

Section 11
Security Research and Development Programs

11.1 BACKGROUND

During the Cold War, DOE had a vigorous research and development (R&D) program for improving nuclear weapon and material security systems. The end of the Cold War and the accompanying decline in support for the nuclear mission have eroded senior decision-makers' support of R&D for improving security systems and led to the deterioration of the once strong R&D management and coordination structures.

11.2 SUMMARY

DOE/NNSA lacks a strategic vision and plan for R&D, procurement, and installation of technologies to improve security across the enterprise. There is no centralized technology component within the department to oversee such a plan. As a consequence, security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without benefit of expert headquarters oversight and complex-wide collaboration. There is no robust technology R&D foundation for an advanced protection strategy.

11.3 OBSERVATIONS

DOE/NNSA lacks a strategic vision or plan for R&D, procurement, and installation of technologies to improve security across the enterprise. As reported by a federal advisory committee,[1] neither DoD nor DOE/NNSA have a robust R&D program that seeks innovative improvements to nuclear security. Over the years, both departments have changed security R&D programs from a "push" orientation, in which managers sought new and innovative ideas and approaches to nuclear security, to a "pull" orientation, in which they wait until a customer identifies a need and the willingness to "pay" for the development. As a result, both rely on older, dated protection technologies, mostly tied to expensive, man-power-intensive security programs.

[1] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U)*, Final Report, April 2002 (Secret).

The DOE *Strategic Security Plan* calls for the establishment of a

> Technology Development and Implementation Plan that will direct the identification, development, acquisition, and application of advanced technologies that will serve as the foundation for an advanced protection architecture.[2]

However, DOE/NNSA has not created a centralized technology component within the department to create such a plan and oversee technological policymaking, research, development, and procurement related to security.

In NNSA, individual laboratories and the Transportation Safeguards Division maintain very small R&D programs, most of which focus on improving existing designs and equipment instead of searching for new and innovative approaches. Some laboratories are engaged in technology R&D programs in their "work for others" programs (such as Department of Homeland Security work.) Self-directed, independent organizations at each site plan and maintain the various security systems. However, little effort has gone into standardizing and improving the systems complex-wide; as a result, each site employs its own unique systems, and the application of similar security resources is not standardized. Most of the limited attempts to standardize security-related items have focused on protective force equipment. Although DOE has quality panels and working groups devoted to this purpose, the sites have realized few technological or labor-saving benefits for security from these initiatives.

Security upgrade initiatives to employ new technologies are inconsistent. Sites are independently engineering upgrades without the benefit of knowledgeable over-sight or direction. Examples are as follows:

- Several sites are in various phases of perimeter upgrades. Rather than taking advantage of the possible synergy from combining upgrade design efforts, each is proceeding independently, possibly duplicating past efforts, wasting resources, and failing to adopt best-of-breed designs and practices.

- One site is planning to design and install a new perimeter intrusion detection system that will also provide denial at the perimeter. No accepted NNSA-wide strategic vision or policy drives this planning decision. Denial at the perimeter has not been demonstrated or been shown superior to denial systems located at the target itself.

On a positive note, some sites have adopted security upgrades that have clearly improved security. One has developed an innovative underground storage for infrequently-used special nuclear material (SNM.) Others have made simple procedural changes which have significantly improved security at little or no cost. One has closed a road to public access; another has permanently closed a site access gate.

---

[2] U.S. Department of Energy, *The Department of Energy's Strategic Security Plan,* March 2003.

Both initiatives have significantly reduced potential vulnerabilities and are good examples of how changes in policy, procedures, or operations can improve security and conserve resources. However, other sites are probably not aware of these initiatives and have not benefited from their example.

There is a prevalent attitude within NNSA that technology is not as flexible as manpower. As requirements change, redeploying security manpower is relatively easy and effective in the short term, but long-term considerations need to include technology. In addition, life safety issues have historically overshadowed the potential use of new security technologies. While safety is essential, a zero tolerance approach to safety deficiencies often precludes safety personnel from working with the operational communities to develop acceptable risk-based approaches to improve security through the use of new technologies.

11.4 RECOMMENDATIONS

1. Reinvigorate nuclear security R&D programs, with an immediate focus on developing improved access delay and denial technologies, including disrupting, disabling, or lethal systems. NNSA should seek to integrate advanced security technologies into facility construction and refurbishment planning processes to anticipate and mitigate emerging threats.

2. Establish a centralized technology component within DOE/NNSA to formulate a Technology Development and Implementation Plan, or equivalent, as authorized in the DOE *Strategic Security Plan.* Assign responsibility, accountability, and resources to this organization to oversee and coordinate policymaking, research, development, procurement, and application of advanced security technologies that can serve as the foundation of an enhanced protection architecture.

3. Collaborate closely with DoD and other government agencies, such as the Technical Security Working Group, to collectively pursue advance security technologies. Leverage R&D initiatives in the "work for others" programs.

4. Consider a reasonable standardization of site security system architecture, design, and implementation, including the security upgrades in progress. NNSA site oversight and headquarters should be involved in each critical decision stage of security upgrade projects. Project rationale and justification should be scrutinized and compared with complex-wide needs and overall direction. This would optimize the use of security up-grade funding and present a clear direction for security strategy.

5. Establish an NNSA R&D security panel to periodically review, evaluate, and critique R&D programs related to security.

Section 12
Nuclear Materials and Waste Storage

12.1 BACKGROUND

A large percentage of DOE/NNSA security resources are devoted to protecting nuclear weapons and special nuclear material (SNM). The wide spectrum of SNM storage facilities—in age, condition and location—drive many of these resource requirements. Because of the evolution of the nuclear weapon infrastructure during the Cold War, the storage facilities tend to be geographically dispersed. SNM is stored at these facilities because of the sites' past and present missions. Radiological waste is also stored at many NNSA sites; protection standards for radio-logical waste are less stringent than those for SNM.

12.2 SUMMARY

DOE/NNSA lack an enterprise-wide plan for SNM consolidation. A lack of collaboration between NNSA and other elements of DOE, such as Environmental Management (EM) and Nuclear Energy (NE), may preclude some secure and cost effective alternatives for consolidation from consideration. DOE/NNSA should seek to make greater use of underground storage. Some radiological waste storage areas may lack adequate protection against sabotage which could cause wide area radiological dispersal.

12.3 OBSERVATIONS

12.3.1 SNM Consolidation

DOE/NNSA has no comprehensive complex-wide SNM consolidation strategy, and NNSA has not coordinated effectively in the past with other program offices in DOE, such as EM and NE, Science and Technology (NE), with respect to underutilized or emptied SNM storage facilities, some of which are underground.

One site has old and deteriorating SNM storage locations, some of which were not designed or intended for long-term storage. Their nature, design, and geographical dispersal make it difficult to provide adequate security against a modern, sophisticated threat. As a consequence, the labor and security technology costs to adequately protect these locations are far greater than those for equivalent, more modern storage facilities. The geographic dispersal also creates multiple potential vulnerabilities. In effect, an aging infrastructure is a primary driver of security resources.

Although isolated efforts have been made to relocate some SNM or design new storage facilities, a detailed, department-wide, comprehensive SNM consolidation study that includes an overall cost-benefit analysis is lacking. Funding requests for SNM transfers and upgrade construction projects could benefit from this type of study.

Past studies have specifically recommended the need to review the existing SNM storage infrastructure and the consolidation of SNM.[1] They found newer, state-of-the-art storage infrastructures that are currently underutilized or empty.

It appears that some SNM is being stored at some DOE/NNSA sites more for convenience than necessity. Some sites perceive that SNM holdings are inextricably tied to their missions. Some quantities of nuclear materials are stored to allow scientists access to their work; however, moving this material to more secure and remote sites, and bringing the scientists and mission to the material would de-crease the number of storage locations and consolidate SNM in more secure, un-populated areas.

A number of underutilized facilities, far from populated areas, could potentially be used to consolidate storage of nuclear weapons and material. The Device Assembly Facility (DAF) at the Nevada Test Site (NTS) is a logical choice. NNSA has only recently begun to relocate SNM to the DAF.

EM's emphasis on closure and objectives related to cleanup and reducing the Department's footprint has hindered the coordination between NNSA and other DOE program offices for evaluating existing SNM infrastructures. Evaluating these facilities—some of which are underutilized, soon to be empty, or empty—may have cost and security benefits. For example, a relatively new 160,000-square-foot, three-level, underground, reinforced-concrete storage facility at the Idaho National Engineering and Environmental Laboratory (INEEL), has never been used.

As far as other underutilized or empty storage vaults, EM could still reach its footprint goals if a DOE EM building could be used to store NNSA SNM, which would entail a transfer of building ownership to NNSA. This effort could potentially also save DOE EM funds if the building(s) could be put to NNSA use thus eliminating the need for EM to commit and spend Deactivation and Decontamination (D&D) funds.

12.3.2 Underground Storage

Insufficient emphasis has been given to the inherent long-term advantages of underground storage. An underground storage vault may initially cost more to build; but, in the long term, the facility is likely to improve security and conserve resources. From a protective system viewpoint, above-ground storage presents additional protection challenges and costs associated with less complicated adversary

[1] *Review of the Special Security Study (for the DOE Security Council),* 1998, and *A Security Architecture for NNSA (A Special Security Study),* 2002.

barrier breaching and greater vulnerability to airborne threats. While some facilities (e.g. the Highly Enriched Uranium Material Facility at the Y-12 Plant) cannot be placed underground for geological reasons, NNSA should seek underground storage wherever possible.

12.3.3 Protection of Radiological Material

DOE/NNSA protection requirements for radiological waste and material storage are minimal or nonexistent. In comparison to other departmental assets such as SNM, classified and other departmental security interests, there is significantly less protection afforded to radiological waste. Protection for radiological waste currently amounts to a fenced boundary area with no consideration given to vehicle barriers, alarms or an armed guard presence, nor is there any requirement for the protective force to develop response plans or conduct performance testing for this type of material. In some cases, assets such as the protective force already exist at a site where radiological materials are stored, but no requirement exists to have them provide any level of protection to this potential adversary target. In some cases there is more access control, detection, and response dedicated to DOE and NNSA owned and operated administrative office buildings than what is applied to radiological waste and material storage areas.

This is not intended to imply that the degree of protection afforded to SNM should be used as a basis for radiological storage. Rather, there is a concern that the lack of protection afforded to radiological materials could make these materials an attractive target to an adversary threat. It is recognized that some of the radiological holdings within the department do not exceed the publicized off-site public dose rates, which precludes them from being identified as a radiological sabotage target. However, even if the material is under this threshold, based upon the type and significant quantities of radiological waste storage areas within the department, a terrorist sponsored wide-area radiological dispersal could cause evacuation of local populations, shut down of site operations for a considerable period of time and considerable cleanup costs.

12.4 RECOMMENDATIONS

1. DOE/NNSA should urgently develop a comprehensive plan for SNM consolidation based on the significant amount of funding that will continue to be spent at NNSA SNM storage facilities that may later become candidates for SNM removal once the consolidation plan is completed. Nuclear weapons and SNM should be consolidated at fewer, better protected sites and where practical, in underground storage sites (e.g. DAF). Where consolidation in underground storage sites is impractical, above-ground structures should be modified to earth-covered structures where feasible to reduce the potential vulnerability from ground or air attack. This effort should receive appropriate emphasis considering

the increased protection required to meet the new DBT. A thorough review of existing infrastructures within DOE to determine if existing structures could be used to consolidate SNM, minimize new construction cost, increase security and potentially save DOE D&D funds should be conducted as part of this plan.

2. In parallel with the nuclear weapons assessment recommended by the End to End Review,[2] direct a feasibility assessment of providing underground storage for all SNM. Evaluate the adequacy of current protection requirements for radiological materials and make cost effective determinations for those areas that can be improved upon.

3. Evaluate the adequacy of current protection requirements for radiological materials and make cost effective determinations for those areas that can be improved upon.

4. Reevaluate the criteria for radiological sabotage to provide sufficient protection strategies for radiological waste against wide-area radiological dispersal.

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System (U)*, Final Report, April 2002 (Top Secret).

Section 13
Security Resources and Requirements

13.1 BACKGROUND

From the beginning, NNSA senior management committed to a planning, programming, budgeting, and evaluation (PPBE) process modeled on the DoD system. A PPBE process uses short- and long-term planning to define program requirements and matches requirements with budgetary resources. The Administrator established the overall objective that the PPBE process become the core management protocol for NNSA.[1]

The PPBE process allows site managers and contractors to define site resource needs and evolve them into unified budgets, including security requirements, be-fore they are evaluated against all program needs at headquarters. Decisions about resources can be made in an integrated manner, taking into account administration policy and the needs of the entire complex. The PPBE process links "long-range planning (*what* NNSA needs to do) with programming (*how* NNSA will accomplish it), with budgeting (obtaining *resources* and applying fiscal *constraints*), and with evaluation (*verifying* that the mission has been accomplished as planned)."[2] NNSA began using the PPBE system for the past three budget years, starting with FY02:

- For FY02, the plan for managing appropriations reflected an integrated NNSA PPBE processes for financial execution, closely tied to milestones and deliverables contained in work authorizations. NNSA began implementing an automated system to streamline budget execution record keeping.

- For FY03, the Office of Management and Budget (OMB) reviewed the NNSA-developed budget, with input from DoD regarding NNSA's weapons-related requirements and associated budgets.

- For FY04, each program component developed an integrated plan. The issuance of the *Five-Year Program and Fiscal Guidance* began the

[1] U.S. Department of Energy, Office of Inspector General, Office of Audit Services, *Audit Report: National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process,* DOE/IG-0614, August 2003. Available from http://www.ig.doe.gov/text/ig-0614.rtg.

[2] Congress, House, Special Oversight Panel on Department of Energy Reorganization Committee on Armed Services, February 26, 2002. Statement of John A> Gordon, Undersecretary of Energy and Administrator for Nuclear Security National Nuclear Security Administration, U.S. Department of Energy. Available from http://www.nnsa.doe.gov.

"programming" step in the NNSA PPBE process. The FY04 budget submitted to Congress fully met the congressional intent of having a PPBE system driving the resource decision process.[3]

By design, NNSA headquarters is responsible for strategic and program planning, budgeting, and oversight of research, development, and nonproliferation activities. Headquarters manages the PPBE process, and the field offices execute it. The process recognizes that each of the five principal program or management elements within NNSA, including Infrastructure and Security, manages program execution and interface with contractors differently.

The *Safeguards and Security (S&S) Program Management Plan* uses formalized planning and measurement techniques that align with the four PPBE phases (Table 13-1).[4]

Table 13-1. Process Alignment with Program Management

PPBE phase	S&S Program Management Plan
Planning	S&S Strategic Plan, S&S Multiyear Program Plan
Programming	S&S Programming and Budget Integration
Budgeting	Work Implementation and Site Change Control
Evaluation	Contractor Performance Evaluation and NA-70 Implementation Phase

13.2 SUMMARY

NNSA has made good progress in implementing the PPBE process, but much remains to be done. The lack of an enterprise approach to security planning, inconsistent site-by-site interpretation and implementation of security resource requirements, lack of collaboration among the participants in the budget process, lack of a centralized budget validation process, and a cumbersome and unresponsive reprogramming process complicate rational resource planning, programming, budgeting, and evaluation to meet evolving security needs.

13.3 OBSERVATIONS

13.3.1 PPBE Implementation

NNSA has made significant progress in the implementation of the PPBE process. The migration to the 5-year PPBE system is forcing more disciplined and consistent

[3] See Note 2.

[4] National Nuclear Security Administration, *NNSA Safeguards and Security Program Management Plan: Work Implementation, Control, and Performance Evaluation at NNSA Sites*, February 2004.

planning in the resource allocation process for security. NNSA is perceived as the model for the rest of DOE, which has been slower to embrace the multi-year PPBE process. However, much remains to be done. The weakest elements in the process are planning and evaluation.

Inconsistent site-to-site interpretation and implementation of security requirements have complicated accurate prioritization of security needs and rational re-source allocation decisions across the NNSA complex. The decision makers, who establish security requirements, the sites, who establish resource requirements, and the resource allocators, who program resources, lack the collaboration needed to ensure that security risk is appropriately balanced across the complex. The lack of an enterprise approach to security and the variation in security policy interpretation and implementation deprive NNSA of the assurance that appropriate priority is accorded to assets needing protection and precludes potential budget savings through economies of scale.

NNSA headquarters has not established a budget validation process. Individual site contractor estimates, which form the basis for budget requests and resource allocation decisions, lacked validation for FY03 and FY04. As identified by the DOE Inspector General, NNSA lacks an independent analysis group to facilitate centralized resource allocation decisions.[5]

Because the NNSA and DOE budgeting processes differ, site contractors are burdened with providing budget and financial information to both organizations.

13.3.2 Security Funding

There is a general debate within DOE/NNSA on the relative merits of direct versus indirect security funding. (DOE has made a recent decision to retain direct line security budgeting.) Direct funding ensures appropriated funds for safeguards and security are not diverted for other purposes; however, direct funding lacks the flexibility to provide additional funds, beyond appropriated levels, to meet emerging needs. In contrast, indirect funding provides great flexibility but lacks congressional visibility in how funds are utilized and creates a potential that safeguards and security may be neglected. While there are pros and cons to each method, the real problem is not direct funding versus indirect funding but lack of sufficient flexibility in reprogramming authority to be sufficiently responsive to emerging security needs. The existing reprogramming process is characterized by the DOE/NNSA senior comptroller officials as a "nightmare." One of the recognized problems is the poor quality of the reprogramming request justifications.

There is a widespread perception that there are insufficient security resources to implement both the new DBT security requirements by FY06 (see Section 10) and the evolving cyber security threat requirements (based on the cyber DBT initiative discussed in Section 5).

[5] See Note 1.

13.4 RECOMMENDATIONS

1. Accelerate the transition to a multiyear PPBE process, which:

   - promotes greater collaboration among the security requirement setters, security resource requesters, and resource allocators;
   - validates site contractor security cost estimates;
   - facilitates more meaningful site-to-site security comparisons;
   - promotes an enterprise view of security priorities and enables a more rational prioritization of security needs; and
   - promotes greater savings from complex-wide security initiatives (for example, from special nuclear material consolidation and migration to underground storage).

   Place particular emphasis on strengthening the planning and evaluation elements of the PPBE process. As part of this initiative, adopt an enterprise-wide, risk-based, security model, as recommended by the Commission on Science and Security, to enable NNSA to better "balance resources, which are limited, and risk, which can never be eliminated."[6] A better understanding of the resource and security tradeoffs would also facilitate creation of a comprehensive NNSA-wide S&S strategic plan, which NNSA envisions as part of the first phase of the PPBE process.

2. Encourage DOE to adopt a similar PPBE process to simplify site contractor budget submissions.

3. Establish an independent analysis group to facilitate centralized resource allocation decisions. This type of group will improve the PPBE process through program reviews, alternatives analysis, and cost estimate validation. In the near term, consider establishing an independent panel to validate the adequacy of funding to implement both the new DBT by FY06 and evolving cyber security threat requirements.

[6] Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary on the Department of Energy Laboratories*, John J. Hamre, commission chair, Anne Wikowsky, project director, April 2002, p.xv. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

4. Seek DOE, OMB, and congressional approval to grant the NNSA Administrator:

   - limited reprogramming authority for the S&S program and
   - authority to submit streamlined formal reprogramming requests directly to OMB and Congress when NNSA needs to transfer security funds beyond the limits of reprogramming authority.

Limited reprogramming authority and streamlined procedures for formal reprogramming requests will go a long way in providing the flexibilities of an indirect funding method but retain the transparency and accountability of the present direct funded budgeting of, and accounting for, security funds.

5. Improve the quality of reprogramming justifications.

Section 14
Security Contracting

14.1 BACKGROUND

In February 2002, NNSA reported to Congress an acquisition strategy to improve accountability. In that report, NNSA stated that it

> must maximize enterprise-wide procurement opportunities and integrate procurement considerations directly with program and project management organizations. To do this, NNSA will develop and implement a simpler, less adversarial contracting approach that capitalizes on the private-sector expertise and experience of its management and operating contractors while simultaneously increasing their accountability for performance on NNSA programs.
>
> The NNSA Office of Procurement and Assistance Management (PAM) is responsible for creating policies and establishing practices that will enable the organization to achieve its goals. ... PAM will (1) maximize enterprise-wide procurement opportunities, (2) ensure the integrity of the acquisition process, (3) enhance performance based contracting and rely on commercial standards for judging contractor support functions, (4) streamline procurement processes, and (5) improve NNSA supply chain and logistics management. NNSA will also create an acquisition corps to develop staff with an enterprise wide perspective of acquisition management.[1]

NNSA has recently proposed a formal rulemaking as the first step in establishing a tailored NNSA acquisition regulation that is independent of the existing DOE acquisition regulation.

Additionally, the Secretary of Energy has recently proposed consideration of alternatives to the existing security contract arrangements.

14.2 SUMMARY

The contractual relationships for security, which NNSA has inherited, are varied and diverse. Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting—with appropriate focus on security as a key element of mangement and operations (M&O) contractor performance—is a very positive, overdue step. NNSA has been operating under the Department of Energy Acquisition Regulation (DEAR);

[1] National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the National Nuclear Security Administration*, February 2002.

however, NNSA requires a unique set of tailored acquisition regulations and a common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

14.3 OBSERVATIONS

The contractual relationships for security, which NNSA inherited, are varied and diverse. The former DOE operations offices established the reporting relation-ships, and the models are still in place at NNSA today. Under the three basic con-tract types, security is the responsibility of one of the following:

- a management and operations (M&O) contractor,
- a contractor that reports directly to the government—separate from the M&O contractor—or
- a subcontractor to the M&O contractor.

The latter two are known as "non-M&O" contracts. In general, government managers and contractors prefer a contract vehicle that establishes a direct relationship between the government officials and contractors responsible for security over one where the security contractor is a subcontractor to the M&O contractor. Government managers particularly tout the benefits of direct security contract management over that of indirect management.

Dissatisfaction with security performance at some sites has led to proposals to consider alternatives to the present arrangement of site security contracts, including:

- a single security contract for the entire NNSA complex rather than separate contracts for each individual site, or
- federalization of site security forces, or at least selected elements of the site security forces, similar to the Transportation Safeguards Division.

Consideration has also been given to using the site security contracts as small business set asides.

Current and past security contracts insufficiently delineate performance expectations. The NNSA move to emphasis on broad, performance-based contracting—with appropriate focus on security as a key element of M&O contractor performance—is a very positive, overdue step.

Until recently, DOE/NNSA has not used the full range of options available for incentivizing security contract performance. It has unnecessarily limited itself to a few incentives (such as award fees and termination), when a wider range could be

used (as identified in the FAR, recommended by the Blue Ribbon Commission Report,[2] and contained in a proposed acquisition regulation under consideration within NNSA). Award fees—because they generally represent a small percentage of contract value, are structured to be regressive in nature, and are relatively predictable—provide limited motivation to contractor behavior. Security contracts that incentivize the contractors with potential time extensions (such as award-term extensions for superior performance) or terminations or recompetition of their contracts for poor performance are far more influential than those with award fee incentives.

Security contractors are tacitly disincentivized from promoting initiatives that would simultaneously improve security and reduce security staffing requirements, such as improved technology or special nuclear material (SNM) consolidation, because the security staffing requirements primarily drive the contract revenue value.

Many of the findings of the Blue Ribbon Panel, which focused solely on DOE laboratory M&O contracts, apply to the existing security contracts within NNSA. Ratings inflation, questionable objectivity of site office ratings, excessive numbers of performance reviews, weak linkage of reviews to compete-or-extend decisions, high cost of competitions, ineffectiveness of incentives, and weak delineation of performance expectations are all characteristic concerns of the pre-sent NNSA security contract arrangements.

Since its inception, NNSA has been operating under the DEAR; however, the DEAR is a one-size-fits-all regulation that legitimately seeks to accommodate the disparate needs of DOE's many diverse program elements—solar energy, fossil energy, energy regulation, site closures, etc. As a result, the DEAR monolithically deals with a host of complex, multifaceted acquisition policies, issues, and approaches. Additionally, the DEAR does not reflect the statutory prohibition against DOE exercising authority, direction, or control over NNSA and its con-tractors (50 U.S.C. 2403).

NNSA's organizational structure and operating philosophy as a corporate enterprise are unique within DOE and require a unique set of tailored acquisition regulations. In addition, NNSA has identified several contracting and contract management initiatives to better control and motivate its laboratories, plants, and test site, such as enterprise acquisitions, supply chain management, and a simplified fee policy and award term incentives. NNSA is also moving toward consolidating disparate systems and guidance into common, standardized policy and practices to enable greater consistency and discipline across its breadth of national security missions.

[2] U.S. Department of Energy, Blue Ribbon Commission on the Use of Competitive Procedures for the Department of Energy Labs, *Competing the Management and Operations Contracts for DOE's National Laboratories,* November 2003. Available from http://www.seab.energy.gov/publications/brcDraftRpt.pdf.

Nearly a year ago, NNSA proposed a formal rulemaking as the first step in establishing a tailored NNSA acquisition regulation independent of the DEAR. This NNSA-unique regulation remains in a process of review and comment within DOE.

Site managers are generally designated as the fee determination official for non-M&O security contracts. Such desegregation leads to perceptions of favoritism and bias because of the close working relationship between site managers and security contractors. Additionally, such designation leads to a wide variation in performance evaluation from site to site.

14.4 RECOMMENDATIONS

1. Continue, with urgency, the development of standardized contracts (both M&O and security where separate) that identify and define desired performance in clear and measurable terms, and utilize the full range of incentives to reward successful performance, including longer-duration security contracts with periodic evaluations to determine an extension or competition. Promote better linkage between performance and the compete-or-extend decision.

2. Evaluate with extreme thoroughness, any proposed alternatives to the pre-sent arrangement of individual site security contracts, commensurate with the gravity of the security mission. Potential risks and benefits need to be carefully assessed. Reject experimental and unvalidated alternatives.

3. Incentivize contractors by rewarding them for initiatives that lead to improved security through improved technology and processes that will en-able lower security staffing costs (such as SNM consolidation).

4. Have DOE formally support NNSA in the creation of an acquisition regulation, independent of the DEAR, tailored to support NNSA's unique mission.

5. Elevate the designation of fee determination official (FDO) for security contracts from site managers to either the NNSA Administrator or the new Associate Administrator for Defense Nuclear Security (NA-70). Such action would:

   - elevate the site contractor's security performance to headquarters level,
   - enhance an enterprise approach to performance evaluations, and
   - mitigate against perceptions of lack of site manager objectivity be-cause site managers work so closely with security contractors.

Section 15
Past Studies

15.1 BACKGROUND

Over the years, dozens of reports from various committees, panels, and DOE organizations have identified and addressed issues the same as or similar to those in this report. Many reports addressed DOE before the formation of NNSA, but several examine the issues since NNSA's creation.

As one report stated,

> Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy direction. As one observer noted in Science magazine in 1994: "Every administration sets up a panel to review the national labs. The problem is that nothing is done."[1]

15.2 SUMMARY

Past studies and reviews of DOE/NNSA security have reached similar findings regarding the cultural, personnel, organizational, policy and procedural challenges which exist within DOE and NNSA. Many of these issues are not new; many continue to exist because of a lack of clear accountability, excessive bureaucracy, organizational stovepipes, lack of collaboration, and unwieldy, cumbersome processes. There are also many other contributing reasons for the failure to implement corrective action. Classified or sensitive information cannot always be shared. Organizational changes and staff reductions impede corporate memory and achievable workload. Lack of prioritization confuses the important with the trivial and the urgent with the non-urgent.

15.3 OBSERVATIONS

Robust, formal mechanisms to evaluate findings, assess underlying root causes, analyze alternative courses of action, formulate appropriate corrective action, gain approval, and effectively implement change are weak to non-existent within DOE/NNSA. Of particular concern, DOE/NNSA has failed to take decisive action to the findings and recommendations of the End-to-End Review and has been slow to

[1] President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

respond to the requirements of [REDACTED]current guidance (which had its origins in the End-to-End Review)[2] despite the gravity of these documents.

Appendix B contains a partial list of past studies and reports addressing similar security subjects to this review.

15.4 RECOMMENDATION

Develop, with urgency, a more robust, integrated DOE/NNSA-wide process to provide accountability and follow-up on security findings and recommendations.

[2] United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Secret).

Bibliography

The panel specifically cites the following documentation in the text of this report. This bibliography represents only a small portion of the documentation the panel reviewed in the course of this assessment.

Commission on Science and Security, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*, John J. Hamre, Commission Chair, Anne Witkowsky, Project Director, April 2002. Executive summary available from http://www.csis.org/css/ExecSummary.pdf.

Congress, House, Special Oversight Panel on Department of Energy Reorganization Committee on Armed Services, February 26, 2002. Statement of John A. Gordon, Under Secretary of Energy and Administrator for Nuclear Security National Nuclear Security Administration, U. S. Department of Energy. Available from http://www.nnsa.doe.gov/.

Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III, December 2002.

Federal Register, Volume 69, Number 129, July 2004. Available from http://edocket.access.gpo.gov/2004/04-15331.htm.

Letter, from Kenneth A. Minihan, President and Chairman of the Board, SASA, to directors of various agencies, February 13, 2004. Available from www.greaterla-isac.com/docs/sasaltrtodci.doc.

Letter, from G. Peter Nanos et al., Laboratory Directors, to Kyle McSlarrow, Deputy Secretary, October 10, 2003.

National Defense Authorization Act for Fiscal Year 2000, Public Law 106-65, Section 3212(b)(2).

National Nuclear Security Administration, "NNSA Announces Security Initiatives for Weapons Laboratories," Press Release, July 8, 2003.

National Nuclear Security Administration, *Functions, Responsibilities and Authorities Manual*, May 2003.

National Nuclear Security Administration, NNSA Policy Letter 14.1, *Cyber Security Program*, September 2003.

National Nuclear Security Administration, *NNSA Safeguards and Security Pro-gram Management Plan: Work Implementation, Control, and Performance Evaluation at NNSA Sites*, February 2004.

National Nuclear Security Administration, *NNSA Safeguards and Security Strategic Plan*, June 2003.

National Nuclear Security Administration, *Report to Congress on the Organization and Operations of the NNSA*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy and Department of Defense, *Joint DOE/DoD Nuclear Weapon Classification Policy Guide*, CG-W-5, January 1984.

U.S. Department of Energy, *The Department of Energy's Strategic Security Plan*, March 2003.

U.S. Department of Energy, DOE Directives System Working Group, Office of Management, Budget and Evaluation, *Report on Streamlining Directives System, presented to the DOE Management Council*, July 23, 2002.

U.S. Department of Energy, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*, DOE Notice 205.4, March 2002.

U.S. Department of Energy, *Identifying and Protecting Official Use Only Information*, DOE Order 471.3, April 2003.

U.S. Department of Energy, *Incidents of Security Concern*, DOE Order 471.4, March 2004.

U.S. Department of Energy, memorandum from Bill Richardson, Secretary of Energy, to John T. Conway, subject: *Providing Revision 1 of the 2000-1 Implementation Plan*, January 19, 2001.

U.S. Department of Energy, memorandum from Edward McCallum, Director, Office of Safeguards and Security, to DOE director distribution, subject: *Enhanced Target Folders Development and Use*, June 4, 1998.

U.S. Department of Energy, memorandum from Robert Card, Under Secretary, to Field Operation Office Directors, subject: *Design Basis Threat*, May 20, 2003

U.S. Department of Energy, memorandum from Spencer Abraham, Secretary of Energy, to Lead Program Secretarial Officers, subject: *Reporting Incidents of Security Concern*, June 14, 2002.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Audit Report: National Nuclear Security Administration's Planning, Programming, Budgeting, and Evaluation Process*, DOE/IG-0614, August 2003. Available from http://www.ig.doe.gov/text/ig-0614.rtf.

U.S. Department of Energy, Office of Management Communications, "Department of Energy Directives Checklist," Directives, Regulations, and Standards, August 2004. Available from http://www.directives.doe.gov/cgi-bin/currentchecklist#POLICY

U.S. Department of Energy, Office of Management, Budget and Evaluation, *RevCom Review and Comment System*, August 2004. Available from http://www.revcom.doe.gov/.

U.S. Department of Energy, *Protective Force Program Manual*, DOE Manual 473.2-2, June 2000.

U.S. Department of Energy, *Reporting Incidents of Security Concern*, DOE Notice 471.3, April 2001.

U.S. Department of Energy, *Safeguards and Security Program*, DOE Order 470.1, September 1995.

U.S. Department of Energy, *Security Incident Notification Report*, Form 471.1.

U.S. Government Accountability Office, *DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623, April 2004. Available from http://www.gao.gov/new.items/d04623.pdf.

United States Nuclear Command and Control System Federal Advisory Commit-tee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

Appendix A
Security Plan Status

Table A-1 shows the status of security plans for the various sites.

Table A-1. DOE NNSA Security Plan Status Summary

Facility	Type	Date
Kansas City Plant	FSP	April 2004
Lawrence Livermore National Laboratory	SSSP	January 2001
Los Alamos National Laboratory	SSSP	September 30, 1999
	FSP	June 18, 2002
• Bio Level 3 (LANL)		
Nevada Test Site	SSSP	August 1, 1998
	FSP	January 28, 2004
• Remote Sensing Laboratory		
Office of Secure Transportation NA-15	SSSP	October 2001
Pantex Plant	SSSP	January 2001
Sandia National Laboratories		
	FSP	January 2003
• California		
	SSSP	November 2000
• New Mexico		
	SSSP	September 7, 2001
• Tonopah Test Range		
Savannah River Site Office (Defense Programs Tritium Facilities)	FSP	February 18, 2004
Y-12 Plant	SSSP	May 20, 2004

Appendix B
Past Studies

This appendix lists past studies that pertain to DOE and NNSA security. They are listed under the sections to which they pertain.

SECTION 2. CULTURE

Chairman, House Armed Services Committee, *Reforming the Department of Energy*, National Security Report Vol. 3, Issue 3, September 1999.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Government Accountability Office, *Improvements Needed In DOE's Safeguards and Security Oversight*, GAO RCED-00-62, Report to the Chairman, Committee on Commerce, House of Representatives—Nuclear Security, February 2000.

U.S. Government Accountability Office, *Major Management Challenges and Program Risks*, GAO-01-246, Performance and Accountability Series, January 2001.

U.S. Government Accountability Office, *Nuclear Security—DOE Faces Security Challenges in the Post September 11, 2001 Environment*, GAO-03-896, Re-port to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, June 2003.

U.S. Government Accountability Office, *Nuclear Security—Improving Correction of Deficiencies at DOE's Weapons Facilities*, GAO RCED 93-10, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Re-sources, Committee on Oversight and Investigations, House of Representatives, November 1992.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Planning at DOE Facilities Incomplete*, GAO RCED-93-14, Report to the Chairman, Subcommittee on Oversight and Investigations, Nuclear Security, December 1992.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

U.S. Government Accountability Office, *Security Issues at DOE and Its Newly Created National Nuclear Security Administration*, GAO RCED-00-123, Testimony before the Subcommittee on Energy and Power and the Subcommittee on Oversight and Investigations Committee on Commerce, Nuclear Security, March 2000.

SECTION 4. SECURITY POLICY

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process*, DOE-IG-0482, September 2000.

U.S. Government Accountability Office, *Improvements Needed In DOE's Safeguards and Security Oversight*, GAO RCED-00-62, Report to the Chairman, Committee on Commerce, House of Representatives—Nuclear Security, February 2000.

U.S. Government Accountability Office, *Nuclear Safety, Potential Security Weaknesses at* [site name] *and Other DOE Facilities*, GAO RCED-91-12, Report to the Congressional Requesters, October 1990.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

SECTION 5. CYBER SYSTEM SECURITY

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Government Accountability Office, *Major Management Challenges and Program Risks*, GAO-01-246, Performance and Accountability Series, January 2001.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

SECTION 6. COUNTERINTELLIGENCE

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

SECTION 7. SITE SAFEGUARDS AND SECURITY PLAN, VULNERABILITY ASSESSMENTS, AND PERFORMANCE TESTING

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy, to All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Protective Force Performance Test Improprieties*, DOE-IG-0602, Audit Report, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process*, DOE-IG-0482, September 2000.

U.S. Government Accountability Office, *Nuclear Security—DOE Faces Security Challenges in the Post September 11, 2001 Environment*, GAO-03-896, Re-port to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, June 2003.

U.S. Government Accountability Office, *Nuclear Security—Improving Correction of Deficiencies at DOE's Weapons Facilities*, GAO RCED 93-10, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Re-sources, Committee on Oversight and Investigations, House of Representatives, November 1992.

U.S. Government Accountability Office, *Nuclear Security—Lessons to Be Learned From Implementing NNSA's Security Enhancements*, GAO-02-358, Report to the Chairman, Committee on Armed Services, Special Oversight Panel on DOE Reorganization, House of Representatives, March 2002.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Safeguards and Security Planning at DOE Facilities Incomplete*, GAO RCED-93-14, Report to the Chairman, Sub-committee on Oversight and Investigations, Nuclear Security, December 1992.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Sub-committee on Oversight and Investigations, December 1991.

SECTION 8. PROTECTIVE FORCE

Booz Allen Hamilton, [site name] *National Laboratory Safeguards and Security Department Review*, November 2003.

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *The Department's Basic Protective Force Training Program*, DOE-IG-0641, Audit Report, March 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Protective Force Performance Test Improprieties*, DOE-IG-0602, Audit Report, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Management of the Departments Protective Forces*, DOE-IG-062, Au-dit Report, March 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Security Overtime at the* [site name] *Operations Office*, ER-B-00-02, Audit Report, June 2000.

U.S. Government Accountability Office, *Key Factors Underlying Security Problems at DOE Facilities*, GAO RCED-99-159, Report to the Chairman, Sub-committee on Oversight and Investigations, Department of Energy, April 1999.

U.S. Government Accountability Office, *Nuclear Security—DOE Actions to Improve the Personnel Clearance Program*, GAO RCED 89-34, Report to the Chairman, Subcommittee on Environment, Energy, and Natural Resources, Committee on Government Operations, House of Representatives, December 1987.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs a More Accurate and Efficient Security Clearance Program*, GAO RCED 88-28, Re-port to the Chairman, Subcommittee on Environment, Energy, and Natural Resources, Committee on Govern Operations, House of Representatives, December 1987.

U.S. Government Accountability Office, *Nuclear Security—NNSA Needs to Better Manage Its Safeguards and Security Program*, GAO-03-471, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives May 2003.

U.S. Government Accountability Office, *Personnel Security—Efforts by DOD and DOE to Eliminate Duplicative Background Investigations*, GAO RCED 92-93, Report to the Chairman, Committee on Armed Services, House of Representatives, 1993.

U.S. Government Accountability Office, *Safeguards and Security Weaknesses at DOE Weapons Facilities*, GAO RCED-92-39, Report to the Chairman, Subcommittee on Oversight and Investigations, December 1991.

United States Nuclear Command and Control System Federal Advisory Committee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

SECTION 9. SECURITY INCIDENTS AND INQUIRIES

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Inspections, *Summary Report on Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self Assessments at [site] National Laboratory*, DOE/IG-0471, Audit Report, May 2000.

U.S. Government Accountability Office, *Key Factors Underlying Security Problems at DOE Facilities*, GAO RCED-99-159, Report to the Chairman, Sub-committee on Oversight and Investigations, Department of Energy, April 1999.

SECTION 10. DESIGN BASIS THREAT IMPLEMENTATION

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs to Re-solve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-623, Report to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, April 2004.

U.S. Government Accountability Office, *Nuclear Security—DOE Needs to Re-solve Significant Issues Before It Fully Meets the New Design Basis Threat*, GAO-04-701T, Testimony to the Chairman, Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform, House of Representatives, April 2004.

SECTION 11. SECURITY RESEARCH AND DEVELOPMENT PROGRAMS

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

SECTION 12. NUCLEAR MATERIALS AND WASTE STORAGE

National Nuclear Security Administration, *Report of the Combating Terrorism Task Force*, February 2002.

President's Foreign Intelligence Advisory Board, Special Investigative Panel, *Science at Its Best, Security at Its Worst*, June 1999. Available from http://cio.doe.gov/Publications/Cyber/pfiab-doe.pdf.

A Security Architecture for NNSA—A Special Security Study (Hagengruber study), March 2002.

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

U.S. Department of Energy, Office of Inspector General, Office of Audit Ser-vices, *Design of the Uranium Storage Facility at the* [site name] *National Security Complex*, IG-0643, Audit Report, March 2004.

United States Nuclear Command and Control System Federal Advisory Commit-tee, Brent Scowcroft, Chairman, *A Critical Independent Assessment of the U.S. Nuclear Command and Control System* (U), Final Report, April 2002 (Top Secret).

SECTION 13. RESOURCES AND REQUIREMENTS

NNSA Security Expertise Study Team, *Strengthening NNSA Security Expertise: An Independent Analysis*, Henry G. Chiles Jr. et al., March 2004.

SECTION 14. SECURITY CONTRACTING

U.S. Department of Energy, memorandum from Deputy Secretary of Energy for All Departmental Elements, subject: *CY 2004 Management Challenges*, January 2004.

18

November 9, 2005

To Catherine A. McMullen, Esq.
Chief, Whistleblower Disclosure Unit
U.S. Office of Special Counsel

The DOE/National Nuclear Security Administration (NNSA) posted an independent security review commonly known as the "Mies Report" on its web site on September 1, 2005. This report echoes the Whistleblower Disclosure made by Richard Levernier in January 2002 (OSC File No. DI-02-0572), specifically corroborating many of the critical issues he identified almost 4 years ago. Left unaddressed, these issues continue to pose a significant threat to U.S. national security. The extraordinary amount of time your office has taken to consider the DOE's inadequate response to Mr. Levernier leaves the OSC increasingly responsible for perpetuating this substantial and specific danger to public health and safety.

The attached chart compares the DOE May 2003 response to Mr. Levernier's whistleblower disclosures with relevant sections in the Mies report. The DOE was quick to write-off his disclosures as "unfounded," "based on information that is dated," and not a substantial and specific danger to public safety and health. It is clear from the attached analysis, however, that issues which the DOE determined were unfounded or dated two years ago still have not been addressed.

It is requested that the Office of Special Counsel evaluate the Mies Report in conjunction with Mr. Levernier's previously submitted comments concerning the DOE response to his Whistleblower Disclosure. The NNSA issued a press release with the Mies Report that contends "the NNSA has implemented more than 70 percent of the recommendations" contained in the report. If so, the OSC should, according to its statutory obligations, reject the DOE's May 2003 report to the OSC as unreasonable and require the Department to provide genuine responses, which demonstrate the changes in agency rules, regulations, or practices (if they have been made) that address the specific disclosures.

Thank you,

Tom Devine, Legal Director
Government Accountablity Project

DOE Response to Levernier May 2003	Mies Independent Review of NNSA Security May 2005
DOE (p. 1): *In general, the allegations do not accurately represent the Department of Energy's current safeguards and security posture. The DOE's safeguards and security efforts have been subject to some of the most intensive formal reviews of any agency in government. These reviews do not support the opinion of the claimant.* *In addition, it is noted that there have been significant changes made to security subsequent to the August 2000 time period, when the NNSA was established. Congress created this organization, in part, to address previous concerns about security in the nuclear weapons complex. Since that time, a number of specific changes have occurred in security throughout the DOE, to include the nuclear weapons complex, which provide additional assurance that the types of issues identified by the claimant are resolved or mitigated. The changes in security approach and protection have been reviewed and validated by independent organizations within the DOE. The DOE continues to ensure a high level of protection of the nuclear materials at DOE facilities.*	**MIES (2-1, 2-2):** In February 2002, NNSA's *Report to Congress* detailed the agency's plan to "integrate security and counterintelligence into NNSA Mission Activities." In fact, NNSA has accomplished many of its stated goals in this area, but its culture still reflects many of the long-standing negative attributes of DOE… NNSA is plagued by a number of cultural problems that, until addressed, will erode its ability to establish and provide security consistent with the gravity of its mission: • Lack of a team approach to security • Disparate views and an underappreciation of security across the enterprise, such that security is not full embraced as integral to mission. • Ingrained organizational relationships that inhibit an enterprise approach to security • A bias against training • An over-reliance on a compliance-based approach to security rather than a more balanced approach using performance-based standards • Lack of trust in the security organization • An absence of accountability.
DOE (p.2): *The overall protection provided to DOE facilities is identified in DOE orders, Manuals and Notices. The basic DOE Order on Safeguards and Security States that the site will be able to defend against a formally defined adversary. This adversary is identified in a classified document entitled the "DOE Design Basis Threat." This document is issued by DOE headquarters, is applicable to all facilities that possess Special Nuclear Material and it forms the basis for developing the protection strategy for DOE sites.*	**MIES (4-2):** The NNSA enterprise lacks a comprehensive strategic security plan. Policy collaboration is lacking: between DOE and DoD, internally within DOE/NNSA headquarters, between headquarters and the sites, and among sites. NNSA does not have adequate staffing to direct policy to the field or facilitate site implementation. In general, security policy is not sufficiently prescriptive and is open to too much individual interpretation in implementation. No effective system is in place for verifying documented security guidance and direction.

DOE (p. 4): *In addition, there is a need for exercise to evaluate new tactics or security approaches. This leads to exercises, in excess of the minimum required, being conducted at each site. The DOE typically conducts many force-on-force exercise each year.*	**MIES (7-11, 8-4):** Some sites fail to comply with DOE policy, which requires at least one exercise quarterly. Some sites conduct several exercises over a year's time, falling short of the quarterly testing requirement. These situations stem in part form scheduled overtime and the manning of higher security condition levels, which have limited the availability of the protective force to train and participate in exercises. Interpretation and application of the quarterly exercise policy vary widely throughout the NNSA complex because of a lack of clear guidance. Some sites do not require the PF to be familiar with or study and analyze response plans; these sites claim that response plan training takes place during force-on-force and tabletop exercises. This training approach is ineffective; at some sites, force-on-force exercise participation is voluntary, exercises are infrequent, and their relation to response plan review is questionable. Site PFs are not conducting enough force-on-force exercises to maintain perishable tactical skills. OA leadership has expressed a similar concern that the PF is stretched too thin across the complex and therefore not conducting enough testing, which leads to the loss of or reduction in perishable tactical skills and reduces overall efficiency.
DOE (p. 8): *The claimant alleges that the "force-on-force" performance tests DOE conducts at its nuclear facilities are deficient in several respects. As a result of the cumulative deficiencies, he contends DOE lacks any reliable basis for concluding that its class "A" nuclear facilities are secure against terrorist attack...* *The DOE sites routinely conduct performance tests of a wide variety of scenarios.*	**MIES (7-8/12):** Some sites need exercises that are more realistic...Training to one particular type of scenario also detracts from realism: although it may begin as a VA worst-case scenario, the more it is exercised, the less worst-case it becomes. When training and the response plan narrowly focus on a scripted scenario, slight variations can challenge the protective force.

DOE (p. 9): *Due to deficiencies and gaps in the force-on-force performance exercises, the claimant alleges that DOE is not adequately prepared to defend the facilities against such an attack. According to the informant, these deficiencies violate DOE Order 470.1, which requires that the protective force be capable of rapid reaction in order to recapture a DOE asset or stop a sabotage attack.* *All DOE sites have a recapture/recovery program as required by Departmental directives. The DOE sites test this recapture/recovery capability. The claimant is correct in his observation that these types of activities are difficult and dangerous situations. The protection strategies fro DOE sites are designed to prevent the site from being placed in a situation where recapture/recovery is needed. Thus, the focus of training is on ensuring that these conditions will not occur. However, DOE does run tests that presume the site has failed in its main goal and must, therefore, perform a recapture/recovery operation. The claimant is apparently not aware of the level of emphasis in these exercises, as several changes to the tactical protection strategies at DOE sites have been made based upon performance test results. The recent testing by the Independent Oversight Office has placed increased emphasis on recapture/recovery, while still ensuring the major focus is on preventing a site from getting into a situation that would require this effort. These changes in tactical protection strategies, combined with additional training and oversight, have increased the level of assurance that the DOE can successfully accomplish this difficult mission...* *...DOE sites have demonstrated their ability to protect against this threat. The DOE is confident that its protective forces are capable of rapid reaction to implement recapture/recovery actions.*	**MIES (8-4,7,8):** Site Recapture and Recovery (RR) planes are nonexistent or inadequate. The sites explain that they focus on a denial-of-access strategy. Denial of access is the primary mission of NNSA sites, and resources and efforts should be dedicated to developing robust denial strategies. However, some sites' reliance on the viability of their denial strategies has precluded them from adequate planning, training, and procurement of appropriate tools for RR should denial fail. Some sites' RR plans incorporate a denial-of-access strategy that inappropriately assumes they will never lose control of the facility. If adversaries gain access to a facility of leave with material, RR programs are critical. Furthermore, the new DBT policy established site responsibility for instituting an RR program. SSSPs and some facility response plans address RR programs and plans, but they vary widely, and some do not fulfill the need for a timely, effective, and viable RR capability or meet the intent of DOE Manual 473.2-2. Some approaches include RR response activities and requirements (spread throughout different response documents) but do not identify one specific response plan for RR of an SNM storage facility or material in un-authorized control. Other RR approaches include tactical options that are rudimentary, very high risk, and not tactically viable. For example, the mechanical and electronic entry techniques used at some sites have not been performance tested or fully evaluated for their effectiveness, and, during iterative site analysis (ISA) processes or OA inspections, some of these techniques have failed testing. DOE Manual 473.2-2 states that when mechanical entry alone will not meet required response times, the site or facility must develop an explosive tactical entry capability... Although the elements of response plan training and testing are critical to effective RR programs, very few sites have conducted actual training or

	testing, and those that have use tabletop activities or walk-through drills. Adversary capabilities continue to increase, but NNSA threat planning lacks dedicated offensive response teams for each site to meet these threats. The manpower-intensive denial-of-access strategy requires numerous protective force personnel dedicated to a material access area in a repel-type posture. Sites say that the resources committed to this effort prevent them from assigning an offensive force as a dedicated, ready, and equipped element for RR response activities.
DOE (p. 11): *MILES exercises are used for a number of specific purposes. These include training of security force personnel in response tactics, validating the strategic and tactical protection approaches used at a site, as well as conducting performance tests. The basic premise of the allegation is that detailed records of all aspects of a MILES exercise are required of all MILES exercises.* *It is not appropriate to attempt to keep the kinds of records identified in the allegation, since the results of a number of the exercises are to modify protection approaches. The testing of the final protection strategy will have all valid information gathered to ensure there is a full understanding of the protection strategy.*	**MIES (7-8, 8-2):** Protocol documents delineating the method and process of site VAs and performance testing are either nonexistent or lack depth. Existing documents lack any detail regarding how tests are identified, approved, conducted, documented, and analyzed and thus are inconsistent across the complex. Very few limited scope performance testing programs have documentation that describes the evaluation of test results and their integration back into the VA process. Many tests do not provide the data that should be sought by the VA analysts… Without an NNSA policy that sets standardized criteria for validating PF operations, determining whether site protective forces can adequately protect DOE Special Nuclear Material and critical assets will remain problematic.
DOE (p. 11, 12): *Additional issues of concern raised by the claimant involve the structure of the performance tests. He notes that the exercises do not replicate real adversary situations. For instance, the exercises lack vehicles driving at high speeds and violence of action simulating actual terrorist capabilities…The tests also fail to compensate for the lack of surprise. The claimant states that the protective forces who serve as the*	**MIES (7-10,11,12, 8-4):** Adversary forces used in most of the force-on-force exercises are not fully representative of the new DBT. [Some sites] conduct training exercises that are scaled down to the point that they don't test the overall protective system capabilities, instead of comprehensive validation exercises that do.

"adversaries" lack the training necessary to simulate terrorist's capabilities in these exercises. *The claimant raised a question on the adversaries that are used for the exercises. The DOE works with the DoD to use personnel who are trained in adversary techniques as part of specific evaluation of DOE sites. The DoD cannot provide sufficient personnel to act as adversaries to all of the DOE exercises. Thus, on-site personnel must conduct many exercises. This gives the exercise adversary inside information that a normal adversary would not have. While this has been argued as an advantage to the adversary, it is an acceptable impact. DoD personnel have been and will continue to be used on selected exercises in order to ensure independence of view.*	[Some sites] practice the exact exercise scenario just days before the exercise. [Some sites] give the adversary force minimal time to plan its attack. Sites seldom use [DoD] special operations personnel as adversary force team members during exercises, preferring to rely on their protective force personnel. Although it is impractical to employ special operations personnel for most exercises, the use of protective force members in most cases can't duplicate the realistic operating experience associated with a professional adversary force. Exercises that use protective force personnel as adversaries often have unrealistic results because these personnel are primarily trained as defenders and lack experience in heavy weapons, explosives, airborne assets, etc. Continued overreliance on the use of protective force personnel as exercise adversaries—rather than more realistic terrorist planning and modus operandi unforeseen by the site—has the potential to create a false sense of security. Force-on-force training at some NNSA sites lacks realism. It is difficult to conduct realistic training exclusively at NNSA sites because the use of explosives, live fire weapons and, at some sites, even simulation type weapons are not allowed in the vicinity of storage facilities for safety reasons.
DOE (p. 14): *The cumulative effect of these deficiencies, according to the source, degrades the value of performance tests. Thus, he asserts that DOE's reliance on the performance tests is misplaced and creates a false sense of security regarding the safety of DOE's class "A" nuclear facilities. He also states that it is misleading for DOE to use the results of these tests as*	**MIES (7-1):** A number of factors—the shortage of experienced VA analysts, increase in work-load resulting from the new design basis threat (DBT), lack of a comprehensive VA training program, overreliance on a few VA tools, and lack of a rigorous, institutionalized VA approach—detract from the validity and consistency of VAs across the NNSA complex. In addition, weaknesses

the basis for its annual report to the President and Congress on the state of DOE's ability to protect its facilities... *Contrary to the informant's allegations, the force-on-force testing by the DOE not only meets its own requirements, it has been noted by independent reviews as some of the best in the country. While the force-on-force testing is very important, the rest of the security efforts (Computer simulations, Tabletop exercises, Limited Scope Performance Test) ensure that the DOE materials and assets are properly protected.*	and wide variations in SSSP limited scope performance testing and force-on-force exercises distort physical security assessments across the complex, promote a false sense of security in selected areas, and complicate prudent allocation of security resources to address potential vulnerabilities.
DOE (p. 15, 16): *The claimant alleges that, overall, oversight of safeguards and security at nuclear sites is increasingly deficient and inaccurate due to the lack of a centralized inspection process managed by headquarters.* *The claimant alleges that the program is unreliable because it is too dependent upon the self-assessment of contractors and local DOE officials. He contends that in order to be effective, the program must incorporate regular, independent inspections by DOE headquarters...* *In general, the claimant misinterprets data and, in other cases, is ignoring existing oversight capability.* *DOE does have a centralized inspection process managed by headquarters.*	**MIES (3-4):** NNSA headquarters has inappropriately delegated virtually all security oversight review, and assistance responsibilities to the site offices, effectively divorcing itself from day-to-day oversight... NNSA's ability to exercise comprehensive, day-to-day security oversight—to monitor security policy implementation, provide critical guidance and advice, assist in the identification of deficiencies and initiation of corrective action, and promulgate lessons learned and best practices across the enterprise—is problematic for a number of reasons.
DOE (p. 16): *The second inspection process appears to be the one the claimant is criticizing. This is the Office of Independent Oversight and Performance Assurance (OA). This office reports directly to the Secretary and provides independent oversight and assessment for all of the DOE for safeguards*	**MIES (3-3,4):** NNSA headquarters has insufficient qualified people to conduct oversight reviews of site security organizations. As a consequence, NNSA relies heavily on OA for support. The lack of security process "ownership" contributes to a lack of accountability within the DOE/NNSA security

and security. This office conducts inspections of those facilities with Category I quantities of Special Nuclear Material on a regular basis.	disciplines… For example, NNSA headquarters and many managers say that responsibility for site security oversight rests with OA. In reality, that office has little if any direct responsibility, authority, and accountability for day-to-day supervision of the NNSA complex.
DOE (p. 18): *The claimant also states that DOE headquarters no longer conducts independent reviews of vulnerability assessments developed by the contractor. Thus, DOE does not independently verify that contractors have identified and mitigated all risks to ensure security at its nuclear facilities. In summary, the claimant alleges that because of the above-cited deficiencies, violations and built-in biases, the survey program is not used effectively and the surveys are not producing reliable information thereby creating a danger to the public health and safety.* *The claimant is relying on dated information…*	**MIES (3-6):** Day-to-day NNSA oversight is lacking as described above. NNSA guidance is vague on the administration of self-assessment programs. As a consequence, NNSA self-assessment programs vary widely in concept and quality. Self-assessment reports range from none to comprehensive. At present the safeguards and security self-assessment program can be characterized as marginally effective at most sites. The survey program has not lived up to its envisioned role. As federal and contractor staffs have been downsized, support for survey programs have diminished. The quality of both surveys and the analytical review of corrective actions have suffered. As a result, analysis of the root cause of deficiencies is often ineffective and corrective actions often address only the most obvious symptoms rather than correcting the underlying fundamental weaknesses. Weak survey programs tend to breed weak self-assessment programs.
DOE (p. 19): *The claimant states that, in addition to these problems, the annual safeguards and security surveys are conducted by employees who perform the assignment only as an adjunct to their regular duties…[However,] Headquarters, other site offices and contractor resources can and have been used to provide the required expertise.*	**MIES (3-3,4):** As identified in the 2004 Chiles report, qualified security personnel—with sufficient certification, training, rotation, and broad experience—are lacking. Both headquarters and the site offices lack security depth and competency.

The claimant appears to be relying on a specific issue that was raised over the reviews conducted by one DOE office in 1999.	

1

Training Courses Completed

Name and Location	Month/Year Attended	Hours	Subject
Management Development Center Sheperdstown, WV	10/99	80	National Security Policy Seminar
Technical Qualification Program HQ DOE	1998		Safeguards and Security
Central Training Academy, Albuquerque, NM	03/97		Crisis Intervention for First Responders
Central Training Academy, Albuquerque, NM	12/96		Explosive Detection
Headquarters, Department of Energy	12/96	16	Sections 3, 6, 7 – General Technical Base Qualification Standard
Classification Authority, HQ DOE	10/96		Secret Derivative Classification Authority
Central Training Academy, Albuquerque, NM	06/96		Violence in the Workplace
Central Training Academy, Albuquerque, NM	03/96		Counterintelligence for Security Professionals
Central Training Academy, Albuquerque, NM	02/96		Introduction to Tactical Intelligence
Central Training Academy, Albuquerque, NM	02/96		Bomb Incident Planning Workshop-Oklahoma City
Central Training Academy, Albuquerque, NM	02/96		Facility Survey and Approval Workshop

Name and Location	Month/Year Attended	Hours	Subject
Central Training Academy, Albuquerque, NM	01/96		Personnel Security Correspondence Course
Central Training Academy, Albuquerque, NM	01/96		Managing a Training Program Workshop
Central Training Academy, Albuquerque, NM	01/96		Introduction to Physical Security Systems Correspondence Course
Central Training Academy, Albuquerque, NM	12/95		Classified Matter Protection Workshop
Central Training Academy, Albuquerque, NM	10/95	40	Vulnerability Assessment Analysis Methods
Headquarters, DOE	05/95		LAN (WIN) for Users
Headquarters, DOE	05/95		DOS for New Users
Headquarters, DOE	05/95		WIN Fundamentals
Headquarters, DOE	05/95		Windows Introduction
Headquarters, DOE	07/94		Conflict Resolution Course
American Management Association	05/94	24	Management Skills and Techniques for New Supv
Headquarters, DOE, Denver, CO	04/94	32	Fundamentals for DOE Operations
U.S. Office of Personnel Management Dallas, TX	03/94	32	Management Seminar

Name and Location	Month/Year Attended	Hours	Subject
American Management Association	03/94	24	Interpersonal Skills
American Management Association	02/94	24	Assertiveness Training for the New or Prospective Manager
U.S. Office of Personnel Management Dallas, TX	02/94	16	People Skills for Supervisors and Managers
American Management Association	02/94	24	Improving your Managerial Effectiveness
American Management Association	01/94	24	Successfully Managing People
American Management Association	01/94	32	Basic Project Management: Planning, Scheduling And Control
American Management Association	11/93	24	Improving Managerial Skills of the New or Prospective Manager
Department of Energy, Rocky Flats Office	08/93		RCRA Awareness, Course 023-440-01
Headquarters Department of Energy Security Evaluations	04/93	16	Safeguards and Security Inspection Concepts
Department of Energy, Rocky Flats Office	03/93	24	Table-Top Vulnerability Analysis Workshop
Department of Energy, Rocky Flats Office	12/92		Respirator Indoctrination, Course 056-284-01

Name and Location	Month/Year Attended	Hours	Subject
Office of Intelligence; Threat Assessment U.S. Department of Energy	11/92	32	DOE's Technical Response to Nuclear Threats Seminar
Department of Energy, Rocky Flats Office	08/92		RCRA Classroom, Course 023-440-01
USAF Special Operations School	08/92	40	Dynamics of International Terrorism
Department of Energy, Rocky Flats Office	06/92		Understanding and Preventing Sexual Harassment
John E. Reid and Associates, Chicago, IL	04/92	16	Advanced Course – Interviewing and Interrogation
Department of Energy, Rocky Flats Office	11/91		Respirator Certification, Course 056-284-01
US DOE Central Training Academy, Albuquerque	09/91	40	Security Crisis Management Training
USAF, Kirtland Air Force Base, NM	06/91	40	Nuclear Weapons Orientation, Advance Course
US DOE Central Training Academy, Albuquerque	03/91	24	Senior Safeguards and Security Managers Forum
US DOE Central Training Academy, Albuquerque	11/89	32	Personnel Security Specialist Training II
Smith and Wesson Academy	09/86	40	Firearms Instructor
Smith and Wesson Academy	09/86	40	Revolvers
Smith and Wesson Academy	11/86	40	Automatic Pistols
USDOE, Savannah River Plant, Aiken, SC	04/84	32	Cost-Plus Award Fee Contracting

Name and Location	Month/Year Attended	Hours	Subject
USDOE Office of Safeguards and Security	05/83	50	Tactical Training Course
International Association of Chiefs of Police Las Vegas, NV	03/83	40	Terrorism and the Nuclear Industry
Morton Grove Police Department, IL	03/83	16	Street Survival Seminar
John E. Reid and Associates, Chicago, IL	06/81	40	Criminal Interrogation & Behavioral Analysis Interviews
US Department of the Treasury Glynco, GA	05/82	32	Legal Review and Arrest Techniques
US Office of Personnel Management Washington, DC	08/82	32	Suitability and Security Adjudication
Sandia National Laboratories, Albuquerque NM.	04/82	40	Simulated Tactical Engagement Exercises
US Office of Personnel Management Chicago, IL	06/81	16	Freedom of Information and Privacy Act
US Department of the Treasury Glynco, GA	04/80	320	Criminal Investigator Training
US Department of the Treasury Glynco, GA	0680	8	Sharpshooter Qualification

Name and Location	Month/Year Attended	Hours	Subject
US Department of the Treasury Glynco, GA	10/80	40	Advanced Law Enforcement Photography
US Department of Agriculture	12/79	80	National Orientation
US Department of Agriculture	11/79	40	Food Stamp Training
US Equal Employment Opportunity Commission	11/78	80	Basic EEO Compliance
State of Illinois Governmental Law Enforcement Training Board, University of Illinois	12/77	38	Law for Police
State of Illinois Governmental Law Enforcement Training Board, University of Illinois	11/75	560	Performance Oriented Basic Law Enforcement

MANAGEMENT DEVELOPMENT CENTER

Shepherdstown, West Virginia

Richard J. Levernier

HAS COMPLETED THE

National Security Policy Seminar

March 15 - 26, 1999

PROGRAM DIRECTOR

DIRECTOR

UNITED STATES DEPARTMENT OF ENERGY

Technical Qualification Program

Rich Levernier

has successfully completed the Technical Qualification Program in the area of

Safeguards and Security

Brooks E. Todd, Acting Director
Field Operations Division
Office of Safeguards and Security

1998

Edward J. McCallum, Director
Office of Safeguards and Security

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard Levernier

has successfully completed

Crisis Intervention for First Responders Interactive Television

Given this 14th day of March, 1997

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard Levernier

has successfully completed

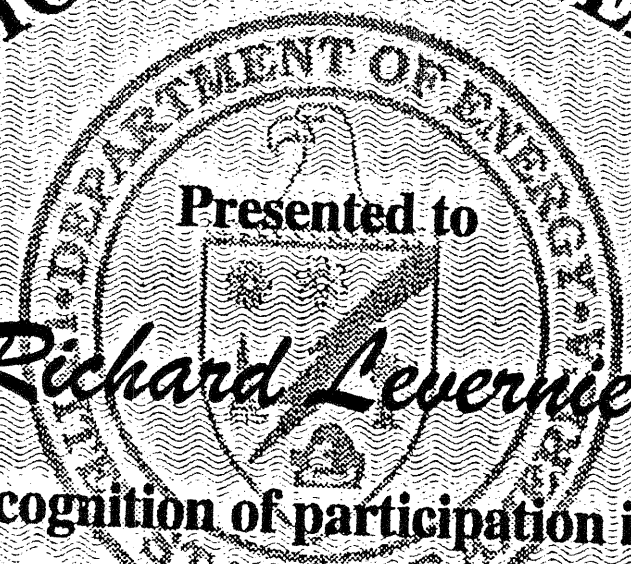
Explosive Detection Interactive Television

Given this 18th day of December, 1996

Director, S&S Central Training Academy

Site Representative

CERTIFICATE OF ATTENDANCE



Presented to

Richard Levernier

in recognition of participation in the

General Technical Base Qualification Standard

(Interactive Television Telecast)

Sections: 3, 6, 7

December 5-6, 1996

Date

Training Officer

Certificate of

CLASSIFICATION AUTHORITY

United States Department of Energy

This is to certify that

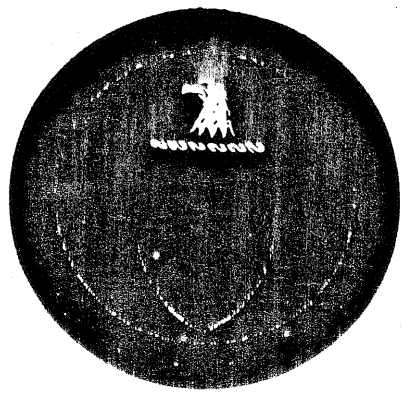
RICHARD J. LEVERNIER

Program Manager, Assessment and Integration
Field Operations Division
Office of Safeguards and Security
Office of Security Affairs

has satisfactorily completed the required training
and is designated as having

SECRET DERIVATIVE CLASSIFICATION AUTHORITY

Director, Office of Declassification



October 1, 1996
Issue Date

October 1, 1999
Expiration Date

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Violence in the Workplace
Interactive Television Training

Given this 27th day of June, 1996

Leonard D. Cook
Director, S&S Central Training Academy

Edward J. McCabe
Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Counterintelligence for Security Professionals

Given this 14th day of March, 1996

Director, S&S Central Training Academy

General Manager, S&S Central Training Academy

Instructor

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Introduction to Tactical Intelligence Interactive Television Training

Given this 29th day of February, 1996

for **Director, S&S Central Training Academy**

Site Representative

United States Department of Energy
Office of Safeguards and Security
Central Training Academy

Presented to

Richard J. Levernier

for attendance at the interactive television training

Bomb Incident Planning Workshop
Oklahoma City Bomb Incident: Lessons Learned

Given this 15th day of February, 1996

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Office of Safeguards and Security
Central Training Academy

Presented to

Richard J. Levernier

for attendance at the

Facility Survey & Approval Workshop
Video Teleconference

Given this 14th day of February, 1996

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Personnel Security Correspondence Course

Given this 26th day of January, 19 96

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Managing a Training Program Workshop Interactive Television

Given this 18th day of January, 1996

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Introduction to Physical Security Systems Correspondence Course

Given this 5th day of January, 19 96

Director, S&S Central Training Academy

Site Representative

United States Department of Energy
Safeguards and Security
Central Training Academy

This is to certify that

Richard J. Levernier

has successfully completed

Classified Matter Protection Workshop Interactive Television

Given this 6th day of December, 1995

Director, S&S Central Training Academy

Site Representative

UNITED STATES
DEPARTMENT OF ENERGY
CENTRAL TRAINING ACADEMY

ALBUQUERQUE, NEW MEXICO

This is to certify that

Richard J. Levernier

has successfully completed

Vulnerability Assessment Analysis Methods

Given this 5th day of October, 1995

Director, Central Training Academy

General Manager, Central Training Academy

Instructor

United States
Department of Energy

Certificate of Training

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed a course in

LAN (WIN) FOR USERS

held at

DOE HEADQUARTERS

Sandra L. Chase
Signature

ADP Training Manager

05/31/95
Date

DOE F 3410.3 (7-92)

United States
Department of Energy

Certificate of Training

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed a course in

DOS FOR NEW USERS

held at

DOE HEADQUARTERS

Sandra L. Chase
Signature

ADP Training Manager

05/24/95
Date

DOE F 3410.3 (7-92)

United States
Department of Energy

Certificate of Training

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed a course in

WIN FUNDAMENTALS

held at

DOE HEADQUARTERS

Sandra L. Chase

Signature

ADP Training Manager

05/23/95

Date

DOE F 3410.3 (7-92)

United States
Department of Energy

Certificate of Training

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed a course in

WINDOWS INTRODUCTION

held at

DOE HEADQUARTERS

Sandra L. Chase
Signature

ADP Training Manager

05/17/95
Date

DOE F 3410.3 (7-92)

Certificate of Completion

RICHARD J. LEVERNIER

Has successfully completed the:

"CONFLICT RESOLUTION COURSE"

July 25, 1994

Ted McAdam Ted McAdam

DEPARTMENT OF ENERGY · UNITED STATES OF AMERICA

AMERICAN MANAGEMENT ASSOCIATION

1.8

Continuing Education Units

awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

MANAGEMENT SKILLS AND TECHNIQUES FOR NEW SUPERVISORS

a concentrated program of study in the field of professional management

MAY 16-18, 1994

Date

David Jagiela

President and Chief Executive Officer

Rose Scalise

Certification Officer

The Continuing Education Unit®

Certification Mark
of the International Association
for Continuing Education and Training

AMERICAN MANAGEMENT ASSOCIATION

The American Management Association is an educational institution incorporated under the New York State Educational Law

United States
Department of Energy

Certificate of Training

This is to certify that

R. LEVERNIER

has satisfactorily completed a course in

FUNDAMENTALS FOR DOE OPERATIONS

held at

Denver, CO April 12-15, 1994

Signature

Charles R. Tierney
Director of Professional and Technical Training and Development

April 15, 1994
Date

DOE F 3410.3 (7-92)

United States

Office of Personnel Management

Dallas Region

CERTIFIES THAT

RICHARD J. LEVERNIER

HAS SUCCESSFULLY COMPLETED
TRAINING IN

MANAGEMENT SEMINAR

CONDUCTED AT

Denver, CO
March 29 -- April 1, 1994

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Edward Vela, Jr.

EDWARD VELA, JR., *Regional Director*

AMERICAN MANAGEMENT ASSOCIATION

1.8

Continuing Education Units

awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

INTERPERSONAL SKILLS

a concentrated program of study in the field of professional management

MARCH 21-23, 1994

Date

President and Chief Executive Officer

Certification Officer

The Continuing Education Unit ®

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law

AMERICAN MANAGEMENT ASSOCIATION

1.8

Continuing Education Units
awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

ASSERTIVENESS TRAINING FOR THE NEW OR PROSPECTIVE MANAGER

a concentrated program of study in the field of professional management

FEBRUARY 28 - MARCH 2, 1994

Date

David Zigarmi
President and Chief Executive Officer

Rose Scalise
Certification Officer

The Continuing Education Unit

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law

United States

Office of Personnel Management

Dallas Region

CERTIFIES THAT

Richard J. Levernier

HAS SUCCESSFULLY COMPLETED
TRAINING IN

PEOPLE SKILLS FOR SUPERVISORS AND MANAGERS

CONDUCTED AT

Denver, Colorado
February 23-24, 1994

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Edward Vela, Jr.

EDWARD VELA, JR., *Regional Director*

AMERICAN MANAGEMENT ASSOCIATION

2.5

Continuing Education Units

awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

IMPROVING YOUR MANAGERIAL EFFECTIVENESS

a concentrated program of study in the field of professional management

FEBRUARY 7-10, 1994

Date

David Sagerman

President and Chief Executive Officer

Rose Scalise

Certification Officer

The Continuing Education Unit®

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law

AMERICAN MANAGEMENT ASSOCIATION

1.8

Continuing Education Units

awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

SUCCESSFULLY MANAGING PEOPLE

a concentrated program of study in the field of professional management

JANUARY 19-21, 1994

Date

President and Chief Executive Officer

Certification Officer

The Continuing Education Unit®

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law

AMERICAN MANAGEMENT ASSOCIATION

2.5

Continuing Education Units

awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

BASIC PROJECT MANAGEMENT: PLANNING, SCHEDULING AND CONTROL

a concentrated program of study in the field of professional management

JANUARY 10-13, 1994

Date

David Sazima

President and Chief Executive Officer

Rose Scalise

Certification Officer

The Continuing Education Unit®

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law

AMERICAN MANAGEMENT ASSOCIATION

1.8

Continuing Education Units
awarded to

RICHARD LEVERNIER

in recognition of satisfactory completion of

IMPROVING MANAGERIAL SKILLS OF THE NEW OR PROSPECTIVE MANAGER

a concentrated program of study in the field of professional management

NOVEMBER 17-19, 1993

Date

David Zigarmi

President and Chief Executive Officer

Rose Scalise

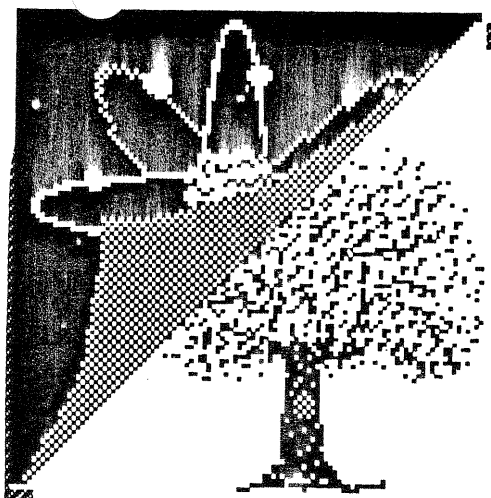
Certification Officer

The Continuing Education Unit®

Certification Mark
of the International Association
for Continuing Education and Training

AMA

The American Management Association is an educational institution incorporated under the New York State Educational Law



Certificate of COMPLETION

This is to certify that

Richard J. Levernier

has satisfactorily completed

RCRA Awareness, Course No. 023-440-01

held at the DOE Satellite Center, Building T371C.

August 10, 1993
Date

J. E. Becker
Instructor's Signature

Rocky Flats Office

Certificate of Attendance

This is to certify that

Richard Levernier

attended the

Forum

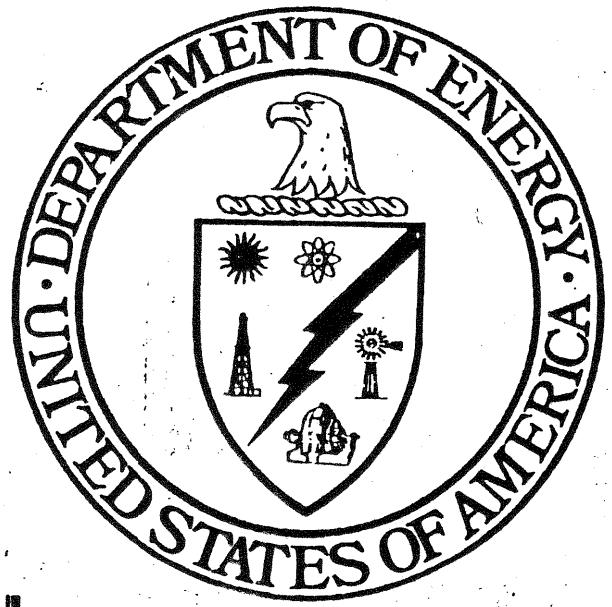
on

Safeguards and Security Inspection Concepts

April 28 & 29, 1993

Scottsdale Arizona

Deputy Assistant Secretary
for Security Evaluations



Certificate

of

COMPLETION

This is to certify that

Richard J. Levernier

has satisfactorily completed the

TABLE-TOP VULNERABILITY ANALYSIS WORKSHOP

March 12, 1993

Date

Lew Goldman

Workshop Director

Rocky Flats Office

Certificate of COMPLETION

This is to certify that

R. J. Levernier

has satisfactorily completed

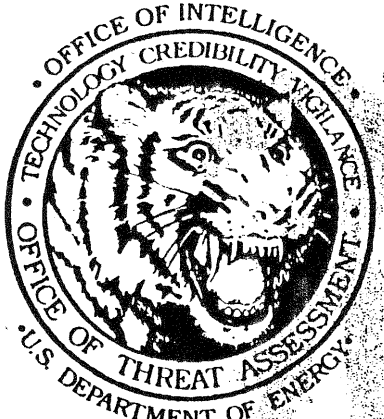
Respirator Indoctrination, Course No. 056-284-01

held at the DOE Satellite Center, Building T371C.

December 11, 1992
Date

Instructor's Signature

Rocky Flats Office



This is to Certify that

Richard Levernier

Has Completed

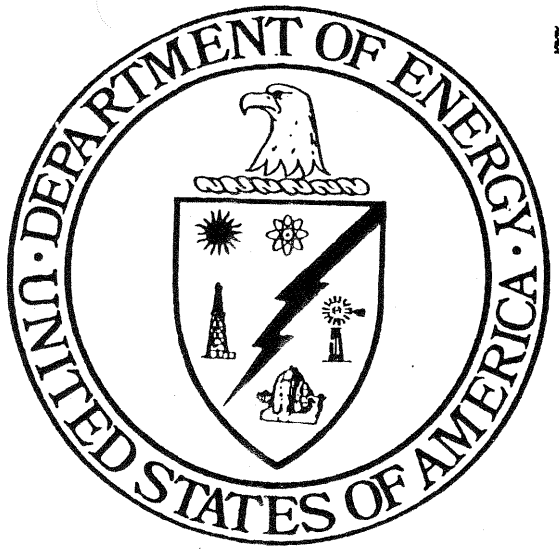
DOE's Technical Response to Nuclear Threats Seminar

November 2 - 5, 1992

Robert A. O'Brien, Jr. Director
Office of Threat Assessment

I believe that until we have looked the tiger in the eye, we shall be in the worst of all possible dangers, which is that we may back into him.

J. Robert Oppenheimer



Certificate of COMPLETION

This is to certify that

Richard J. Levernier

has satisfactorily completed

RCRA Classroom, Course No. 023-440-01

held at the DOE Satellite Center, Building 115.

August 26, 1992

Date

Patty Ashford

Instructor's Signature

Rocky Flats Office

The USAF Special Operations School

Certifies

GM-15 RICHARD J. LEVERNIER, 350-42-1453

has completed the

DYNAMICS OF INTERNATIONAL TERRORISM
CLASS 92H, 10 - 14 AUGUST 1992

and is hereby awarded this Diploma

Michael M. Flynt

MICHAEL M. FLYNT, Colonel, USAF
Commandant

Certificate of Training

This is to certify that

Richard Levernier

has satisfactorily completed a course in

Understanding & Preventing Sexual Harassment

held at

Rocky Flats Office, Colorado

George Cannata

June 8, 1992

Date

DOE F 3410.3
(4-82)

John E. Reid and Associates

Chicago, Illinois

hereby certifies that

Richard J. Levernier

Attended and successfully completed an

Advanced Course

on

The Reid Technique

of

Interviewing and Interrogation

April 9-10, 1992

Daniel A. Malloy
Course Instructor

James J. Bobal
Course Instructor

Certificate of COMPLETION

This is to certify that

Richard J. Levernier

has satisfactorily completed

Respirator Certification, Course No. 056-284-01

held at the DOE CBT Satellite Center, Building 115.

November 26, 1991

Date

Kathy Crawford

Instructor's Signature

Rocky Flats Office

UNITED STATES
DEPARTMENT OF ENERGY
CENTRAL TRAINING ACADEMY

ALBUQUERQUE, NEW MEXICO

This is to certify that

Richard J. Levernier

has successfully completed

SECURITY CRISIS MANAGEMENT TRAINING

Given this 20th day of September, 1991

Director, Central Training Academy

General Manager, Central Training Academy

Instructor

The United States Air Force

CERTIFIES THAT

Mr. Richard J. Levernier
350-42-1453

HAS SUCCESSFULLY COMPLETED THE

NUCLEAR WEAPONS ORIENTATION - ADVANCED COURSE
COURSE NUMBER: G3OZP4054-000
KIRTLAND AIR FORCE BASE, NEW MEXICO 87117-5000

AND IS HEREWITH AWARDED THIS

Certificate of Training

James L. Donahue

JAMES L. DONAHUE, Lt Col, USAF
Commander
Interservice Nuclear Weapons School

14 June 1991
DATE

UNITED STATES
DEPARTMENT OF ENERGY
CENTRAL TRAINING ACADEMY
ALBUQUERQUE, NEW MEXICO

This is to certify that

Richard J. Levernier

has successfully completed

Senior Safeguards and Security Managers' Forum

Given this 6th day of March, 1991

Donald S. Cook
Director, Central Training Academy

Ted E. Leonard
General Manager, Central Training Academy

Instructor

UNITED STATES
DEPARTMENT OF ENERGY
CENTRAL TRAINING ACADEMY
ALBUQUERQUE, NEW MEXICO

This is to certify that

Richard J. Levernier

has successfully completed

PERSONNEL SECURITY SPECIALIST TRAINING II

Given this 8th day of December, 1989

Director, Central Training Academy

General Manager, Central Training Academy

Instructor

Smith&Wesson
Academy

Certificate of Achievement

This is to certify that Richard J. Levernier has satisfactorily completed all required course work for Firearms Instructor.

Director

September 26, 1986

Date

Smith&Wesson
Academy

Certificate of Achievement

This is to certify that Richard J. Levernier has satisfactorily completed all required course work for Revolvers.

Director

September 19, 1986
Date

Smith & Wesson
Academy

Certificate of Achievement

This is to certify that Richard J. Levernier has satisfactorily completed all required course work for Auto-Pistol.

Director

November 7, 1986

Date

Certificate of Achievement

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed the requirements for

U.S. DEPARTMENT OF ENERGY
COST-PLUS-AWARD-FEE CONTRACTING

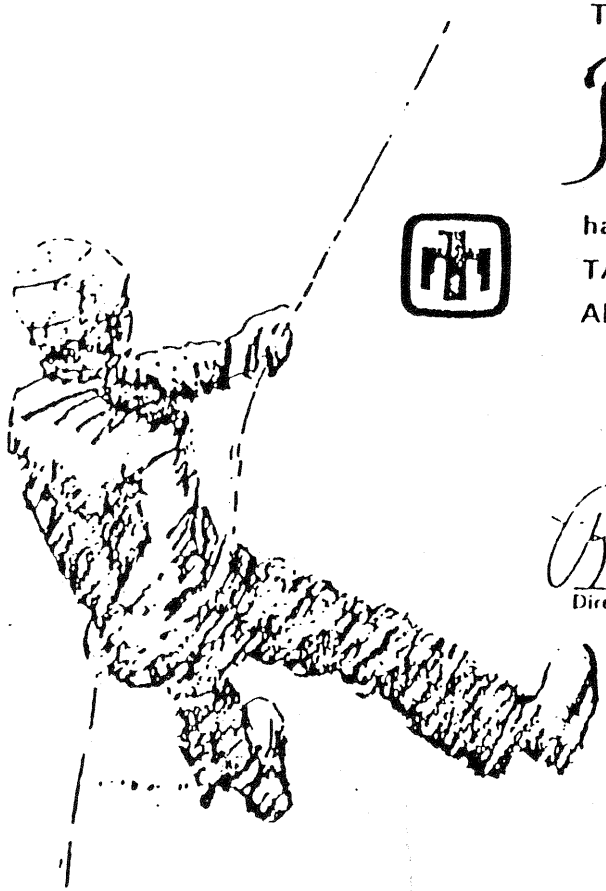
given at

AIKEN, S.C.

17 APRIL , 84

EDWARD R. PULSIFER, PRESIDENT

UNITED STATES DEPARTMENT OF ENERGY
Office of Safeguards and Security



This is to certify that

Richard J. Levernier

has completed a fifty (50) hour concentrated
TACTICAL TRAINING COURSE supported by Sandia National Laboratories,
Albuquerque, New Mexico. Date May 13, 1983.

Ralph E. Cauble
Director, Office of Safeguards & Security

Instructor

The International Association of Chiefs of Police

Certificate of Training

This is to certify that

RICHARD LEVERNIER

has successfully completed training in

TERRORISM AND THE NUCLEAR INDUSTRY

Given this 4TH *day of* MARCH *19* 83

At LAS VEGAS, NEVADA

Executive Director
International Association of Chiefs of Police

Program Director
International Association of Chiefs of Police

Morton Grove Police Department

This certifies that

RICHARD J. LEVERNIER

has satisfactorily completed the

STREET SURVIVAL SEMINAR

a 16-hour training course in firearms tactics, patrol procedures, and officer survival awareness

Conducted in conjunction with
Calibre Press, Inc.

Awarded at Morton Grove, IL, this 9th day of March, 1983

Dennis Anderson
Instructor

David S. Tracy
Instructor

John E. Reid and Associates

Chicago, Illinois

Hereby Certifies That

Richard J. Levernier

Attended and successfully completed a Specialized Short Course

on

Criminal Interrogation

and

Behavioral Analysis Interviews

at

Reid College

June 22-26, 1981

John E. Reid

President, John E. Reid and Associates

Joseph P. Buckley

Course Director

Department of the Treasury

Federal Law Enforcement Training Center

Glynco, Georgia

Certificate of Completion

This certifies that

Richard J. Lenernier

has successfully completed a course of instruction in Legal Review and Arrest Techniques.

May 15, 1982

Date

THE DEPARTMENT OF THE TREASURY 1789

Acting Director

united states of america

office of personnel management

certificate of training

This is to certify that

RICHARD J. LEVERNIER

Has attended the SUITABILITY AND SECURITY ADJUDICATION

Given in WASHINGTON, D.C.

Name Jerry Walsh, Manager

Title Personnel Management Training Center, WED

Date August 17-20, 1982

OPM Form 647-A January 1978

Certificate

SECURITY FORCES EXPERIMENTATION & EVALUATION

This is to certify that

RICHARD LEVERNIER

has participated in Simulated Tactical Engagement Exercises using the Multiple Integrated Laser Engagement System sponsored by the Sandia National Laboratories "SFEE" Division, Albuquerque, New Mexico.

JAMES J. DAVIS — 4/19/82
date

R. D. MILLER — 4/19/82
date

United States

Office of Personnel Management

GREAT LAKES REGION

Presents This Certificate of Training
To

RICHARD J. LEVERNIER

for having successfully completed

FREEDOM OF INFORMATION AND PRIVACY ACT

June 17-18, 1981
Chicago, IL

Conducted by the

REGIONAL
Great Lakes TRAINING
CENTER

DIRECTOR

Department of the Treasury

Federal Law Enforcement Training Center

Glynco, Georgia

This certifies that

RICHARD J. LEVERNIER

has successfully completed all requirements

for graduation in

CRIMINAL INVESTIGATOR TRAINING CLASS 831

June 4, 1980

Date

Program Manager

Federal Law Enforcement Training Center

Glynco, Georgia

SHARPSHOOTER

This certifies that

RICHARD J. LEVERNIER

has qualified as Sharpshooter on the Practical Pistol Course

June 4, 1980

Date

Chief, Firearms Training

Department of the Treasury

Federal Law Enforcement Training Center

Criminal Investigator Training Program

Glynco, Georgia

This certifies that

RICHARD J. LEVERNIER

has completed the requirements for graduation in the course of instruction in Advanced Law Enforcement Photography.

PROGRAM MANAGER
(Criminal Investigator Training)

October 6 - 10, 1980
Date

UNITED STATES DEPARTMENT OF AGRICULTURE

Certificate of Training

This is to certify that

RICHARD J. LEVERNIER

has satisfactorily completed

NATIONAL ORIENTATION

given by

OFFICE OF INSPECTOR GENERAL

DECEMBER 14, 1979

INSPECTOR GENERAL

UNITED STATES DEPARTMENT OF AGRICULTURE

Certificate of Training

This is to certify that

RICHARD LEVERNIER

has satisfactorily completed

FOOD STAMP TRAINING

given by

OFFICE OF THE INSPECTOR GENERAL

NOVEMBER 9, 1979

INSPECTOR GENERAL

Equal Employment Opportunity Commission

Training Certificate

Awarded To

Richard J. Levernier

In recognition of successful completion

of the course in

Basic Compliance

Oct. 23 - Nov. 3, 1978

DATE

Preston David

EXECUTIVE DIRECTOR

UPTC CAMPAIGN
Room 359 · Armory Building
Champaign, IL 61820
(217) 333-2537

NORTHERN CENTER
1415-17 Center Circle Drive
Downers Grove, IL 60515
(312) 620-5650

URBANA
(217) 333-6522

POLICE TRAINING INSTITUTE

UNIVERSITY OF ILLINOIS · Office of the Associate Vice President for Public Service

January 6, 1978

Chief Norman W. Glauner
Morton Grove Police Department
8525 Callie Avenue
Morton Grove, Il 60053

Dear Chief Glauner:

I am pleased to inform you that Officer Richard J. Levernier has satisfactorily completed the 38 hour course entitled Law for Police conducted by the Police Training Institute from December 12 to December 16, 1977. This officer's final grade for the course is 96 and absences from class totalled 0 hours. This officer also met other requirements of the Illinois Local Governmental Law Enforcement Officers Training Board and the Board has received a report on this officer's completion of this course.

You are certainly to be commended for affording this officer an opportunity for specialized training beyond the Basic level. It will continue to be the policy of this Institute to make available as many opportunities for specialized training as are possible. We look forward to the continuing challenge of serving the training needs of your department.

Sincerely,

Clifford W. Van Meter
Director

CWVM:ms

POLICE TRAINING INSTITUTE

UNIVERSITY OF ILLINOIS

Awards This Certificate To

RICHARD J. LEVERNIER

In Recognition of Satisfactory Completion of

LAW FOR POLICE

Conducted at DOWNERS GROVE, ILLINOIS
DECEMBER 12 - DECEMBER 16, 1977

John B. Claar
Associate Vice-President
for Public Service

Clifford W. Von Mutter
Director
Police Training Institute

State Of Illinois

CERTIFICATE

awarded to RICHARD J. LEVERNIER

by the ILLINOIS LOCAL GOVERNMENTAL LAW ENFORCEMENT OFFICERS TRAINING BOARD

In recognition of the successful completion of the 560 hours course in

PERFORMANCE ORIENTED BASIC LAW ENFORCEMENT

at UNIVERSITY OF ILLINOIS from AUGUST 18 to NOVEMBER 21, 1975

SCHOOL DIRECTOR

CHAIRMAN OF BOARD

EXECUTIVE DIRECTOR

2

LEVERNIER, Richard J.

Performance Related Documentation

February 2000	Monetary Award for Special Act or Service from SO-1
March 1999	Annual Performance Appraisal Rating of "Outstanding"
October 1998	Joint Staff Integrated Vulnerability Assessment Team Certificate
February 1998	Annual Performance Appraisal Rating of "Outstanding"
April 1995	Letter, Yucca Mountain Request for Technical Assistance
January 1995	Monetary Award for Superior Job Performance Certificate
November 1992	Outstanding Performance Appraisal Certificate
June 1992	Letter of Commendation from the General Manager, EG&G, Rocky Flats
April 1992	Letter of Commendation from the Manager, DOE Rocky Flats
April 1992	Outstanding Performance Appraisal Certificate
April 1992	Certificate of Commendation from the Manager, DOE Rocky Flats
June 1991	Letter of Commendation from the Manager, DOE Rocky Flats
May 1991	Letter of Commendation from the General Manager, EG&G, Rocky Flats
December 1988	Monetary Award for Superior Job Performance Certificate
December 1987	Monetary Award for Superior Job Performance Certificate
June 1986	Certificate of Appreciation from Assistant Secretary for Defense Programs
February 1985	Letter of Appreciation from Assistant Secretary for Defense Programs
August 1984	Annual Performance Appraisal Rating of "Outstanding"
June 1984	Special State Constable Commission from the Governor of South Carolina
March 1983	Cash Award for Special Act or Service from the Manager, DOE Chicago
May 1980	Certificate of Merit from Acting Inspector General, US Department of Agriculture

United States
Department of Energy

Monetary Award for Special Act or Service

Presented to

Richard J. Levernier

In recognition of your significant contributions in leading a team to review the Rocky Flats Site Safeguards and Security Plan. Your dedicated efforts and expertise have been instrumental in protecting the national safeguards and security interests of the United States.

Eugene E. Habiger, GENERAL, USAF (RETIRED)
Director
Office of Security
and Emergency Operations

February 2000

DOE F 3450.4 (10-94)

(All Previous Editions are Obsolete)

1999

PERFORMANCE RECORD

FOR

PERFORMANCE MANAGEMENT AND RECOGNITION SYSTEM EMPLOYEES

AND

PERFORMANCE MANAGEMENT SYSTEM EMPLOYEES

NAME OF EMPLOYEE RICHARD J. LEVERNIER

SOCIAL SECURITY NUMBER 350-42-1453

POSITION TITLE/PAY PLAN/SERIES/GRADE SECURITY SPECIALIST, GS-080-15

ORGANIZATION & LOCATION ASSESSMENT AND INTEGRATION STAFF, NN-513

DOE F 3430.7 (4-86) **U.S. Department of Energy**
(All Previous Editions Are Obsolete)

CERTIFICATIONS

Section A CERTIFICATION OF DISCUSSION & ISSUANCE OF ELEMENTS/STANDARDS

a. I have received a copy of my elements/standards for this appraisal period and have been provided an opportunity to discuss them with the rating official. (Employee may provide comments on the reverse side of this form).

CHECK IF APPLICABLE

b. ✓ The elements/standards used in the Performance Appraisal Plan for the previous annual rating period will remain in effect during this rating period, which begins 01/01/98 and ends 12/31/98

Richard J. Levernier — 4-15-98
(Signature of Employee) — *(Date)*

Brooks E. Todd, Acting Director, NN-513 — 4/15/98
(Signature of Rating Official) — *(Date)*

Edward J. McCallum, Director, NN-51 — 4/15/98
(Signature of Reviewing Official) — *(Date)*

Section B CERTIFICATION OF PROGRESS REVIEW

Performance and progress to date have been discussed with the employee in accordance with DOE 3430.3A.

Richard J. Levernier — 8-31-98
(Signature of Employee) — *(Date)*

Brooks E. Todd — 9/21/98
(Signature of Rating Official) — *(Date)*

DOE F 3430.7 (4-86)
(All Previous Editions Are Obsolete)

U.S. Department of Energy

CERTIFICATIONS

Section A CERTIFICATION OF DISCUSSION & ISSUANCE OF ELEMENTS/STANDARDS

a. I have received a copy of my elements/standards for this appraisal period and have been provided an opportunity to discuss them with the rating official. (Employee may provide comments on the reverse side of this form).

CHECK IF APPLICABLE

b. ✓ The elements/standards used in the Performance Appraisal Plan for the previous annual rating period will remain in effect during this rating period, which begins 01/01/97 and ends 12/31/97

Richard J. Levernier — *(Signature of Employee)* — MARCH 20, 1997 *(Date)*

Brooks E. Todd, Acting Director, NN-513 — *(Signature of Rating Official)* — 3/21/97 *(Date)*

Edward J. McCallum, Director, NN-51 — *(Signature of Reviewing Official)* — 3/24/97 *(Date)*

Section B CERTIFICATION OF PROGRESS REVIEW

Performance and progress to date have been discussed with the employee in accordance with DOE 3430.3A.

Richard J. Levernier — *(Signature of Employee)* — JUNE 20, 1997 *(Date)*

Brooks E. Todd — *(Signature of Rating Official)* — 4/20/97 *(Date)*

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial) 2. Pay Plan/Series Grade 3. Rating Period

LEVERNIER, RICHARD J. GS-080-15 From: 11|26|95 To: 12|31|96

4. Check One:
_X_ Annual Rating of Record ___ Detail ___ Position Change ___ Temporary Promotion
___ Other, specify:

PERFORMANCE ELEMENT Number 1 of 8 ✓ Critical ___ Noncritical

Accountability to senior management of the Office of Safeguards and Security (OSS), Office of Security Affairs, and the Department of Energy (DOE).

PERFORMANCE STANDARDS

MARGINAL
Lacks understanding of the needs of senior management. Informs top management of routine problems arising out of the day-to-day activities and consults management concerning proposed routine actions. Normally responsive to management directions and requests. Usually informs management of significant events or occurrences in a timely fashion, but sometimes fails to do so. Occasionally fails to provide adequate support to senior management's programs or priorities as evidenced by failure to convey information or supporting rationale to subordinates, contractors, or other individuals. Sometimes the incumbent's failure to abide by established priorities detracts from program success.

FULLY SUCCESSFUL
Advises management of significant occurrences or developments and trends indicating potential for serious problems. Anticipates senior management's needs. Reporting is timely and objective. Routinely responsive to management directions, requests, and needs. Proposes reasonable solutions or alternatives to prevent or minimize negative consequences. Demonstrates loyalty and team spirit in actions taken and performance of duties.

OUTSTANDING ___ Generic Standard will be used. _X_ Generic standard will not be used.
Recognized as an exceptionally competent professional; consistently responsive to management directions, requests, and needs. Highly adept at discerning what information senior management requires to perform effectively, and at providing pertinent information in a succinct form and timely fashion. Unfailing in providing strong support to senior management positions. Effectively demonstrates personal loyalty and fosters team spirit among fellow workers and subordinates.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 2 of 8 ✓ Critical ___ Noncritical

Plans, organizes, directs, and controls staff taskings and work efforts related to DOE safeguards and security assessment and integration issues.

PERFORMANCE STANDARDS

MARGINAL

Assigned tasks are usually monitored to completion and generally meet guidance regarding scope, reporting, timeliness and other specified conditions. Occasional supervisory involvement is required to ensure completion of priority action items. Work products must be reviewed thoroughly by supervisor to ensure consistent adherence to quality standards. Approaches to management tasks sometimes indicate inadequate planning or organization. Occasionally incumbent must be reminded to manage or apply allocated funding or other resources judiciously. Incumbent sometimes fails to coordinate resource requirements adequately, balance workloads or provide clear direction to team members or contractors where appropriate.

FULLY SUCCESSFUL

Incumbent effectively plans and assigns work associated with taskings. Coordinates resource requirements as appropriate. Sets priorities and establishes schedules for work completion. Ensures timely performance of work, makes changes in work assignments to balance work loads and meet schedules. Priority action items and taskings are complete on time or corrective action is taken at appropriate times. Work products reflect creative thought, thorough research and analysis of issues and problems, attention to detail, and adherence to standards, as appropriate. Allocated funds and other resources are effectively applied to meaningful tasks and are professionally managed.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

Incumbent displays superior initiative in identifying and addressing substantive issues and problems not assigned by supervisor. Work efforts are consistently planned and executed to provide orderly flow of high quality products to fulfill tasking and enhance the safeguards and security program. Exceptional leadership results in a sustained high degree of staff productivity. Incumbent's grasp of responsibilities and actions taken clearly reflect exceptional competence and demonstrated ability to assume more demanding responsibilities.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial) — 2. Pay Plan/Series Grade

LEVERNIER, RICHARD J. — GS-080-15

PERFORMANCE ELEMENT Number 3 of 8 ✓ Critical ____ Noncritical

Sets performance standards and reviews the performance of team members.

PERFORMANCE STANDARDS

MARGINAL

Higher level of management involvement is sometimes required to resolve day-to-day team member problems. Meets periodically or upon request with assigned personnel to discuss and establish priorities and performance expectations. Communicates OSS management policies and initiatives. Training and developmental needs of team members are discussed. Evaluates team members' performance. Performance of duties is generally adequate but incumbent sometimes fails to establish priorities, convey information or provide necessary guidance to subordinates thereby contributing to morale problems.

FULLY SUCCESSFUL

Informally appraises team members' performance at least quarterly and accomplishes formal appraisals as required. Team members' career goals are discussed and individual developmental needs are discussed and accommodated within government interests, budgetary constraints and scheduling considerations. Ensures recognition of exceptional work by team members and initiates appropriate action to address performance problems.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

In addition to Fully Successful, consistently achieves exceptional success in motivating team members to strive for excellence in the accomplishment of their duties. Identifies team personnel who evidence promising developmental potential and seek assignments which will benefit both the individuals and the organization and makes recommendations to Division Director. Incumbent continually strives to improve the productivity of individuals within the team; displays creativity and initiative in devising and recommending motivational programs.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 4 of 8 ✓ Critical ___ Noncritical

Provides expert advice and planning guidance on the development, review, and analysis of facility Master Safeguards and Security Agreements (MSSAs) that cover safeguards and security protection of operations at nuclear weapons design laboratories, nuclear material weapons and production facilities, and nuclear weapons testing installation.

PERFORMANCE STANDARDS

MARGINAL

The incumbent sometimes fails to adequate advice and assistance to field offices in the integration of MSSAs into the protection programs at the specific sites. May show insufficient knowledge of DOE and other Government regulations and directives pertaining to safeguards and security as evidenced by recommendations that do not fully address critical issues and/or site-specific considerations.

FULLY SUCCESSFUL

Consistently furnishes expert advice and planning guidance on the development, review, and analysis of facility MSSAs. The incumbent functions as a focal point for integration activities to establish formal MSSAs between Headquarters and field office managers on protection programs at each DOE site based upon site-specific considerations.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

The incumbent provides unusually positive and effective leadership in the formulation and implementation of MSSAs for DOE nuclear weapons facilities that are fully compatible with DOE and other Governmental regulations pertaining to safeguards and security at facilities critical from the standpoint of national security. Advice and guidance is regularly recognized as authoritative and is readily accepted due to the technical soundness of recommendations and advice.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 5 of 8 ✓ Critical ___ Noncritical

Maintains comprehensive knowledge of analysis and assessment methodologies and techniques. Ensures exploitation of new techniques and technologies that contribute to mission accomplishment in effective ways.

PERFORMANCE STANDARDS

MARGINAL

The incumbent occasionally shows limited knowledge of state-of-the-art safeguards and security concepts and technology. Shows reluctance to take action to ensure the integration of new techniques and technologies that could enhance achievement of mission objectives. The incumbent may not adequately present to senior management the need for and the benefits of incorporating new safeguards and security technologies into protection programs for field operations.

FULLY SUCCESSFUL

The incumbent effectively ensures the exploitation of new techniques and technologies that contribute to mission accomplishment. Applies knowledge of state-of-the-art safeguards and security concepts and technologies in reviewing and recommending adjustments to protection programs for DOE operations offices and cognizant facilities. The incumbent generally presents sound and convincing cases to senior management regarding the need for and the benefits of using new safeguards and security technologies.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

Recommendations regarding the integration of new safeguards and security concepts and technologies into field operations protection program are nearly always accepted by senior management because of the incumbent's stature as a widely-recognized authority in the discipline. The incumbent regularly shows how new methods would enhance safeguards and security objectives at a cost savings to the Government.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial) LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade GS-080-15

PERFORMANCE ELEMENT Number 6 of 8 ✓ Critical ___ Noncritical

Evaluates, supports, and defends safeguards and security improvement projects throughout the planning and budget cycles. Provides a focal point within DOE to ensure prioritization of safeguards and security projects and activities.

PERFORMANCE STANDARDS

MARGINAL

The incumbent provides superficial assessments of safeguards and security vulnerabilities and deficiencies that, in some cases, detract from efforts to assign appropriate priorities and resources to address such problems. May not recognize how cost saving may be achieved through safeguards and security standardization at some DOE sites. The incumbent sometimes does not effectively coordinate safeguards and security projects and improvement activities with other DOE elements. May not consistently monitor the status of safeguards and security implementation and improvement activities.

FULLY SUCCESSFUL

The incumbent is conscientious in overseeing the status of safeguards and security implementation and improvement activities. Coordinates projects and improvement endeavors with other DOE elements. Efforts contribute to valid identification of safeguards and security vulnerabilities and deficiencies and that such problems receive requisite attention and commitment of resources.

OUTSTANDING ___ Generic standard will be used. _X_ Generic standard will not be used

The incumbent's evaluations of safeguards and security vulnerabilities and deficiencies are consistently thorough and materially contribute to the assignment of appropriate prioritization and resource commitments through the planning and budget cycles, resulting in substantial improvement in protection programs. Maintains stature as an expert in safeguards and security implementation and improvement activities, and is recognized by other DOE elements as an authority whose coordination efforts, assessments, and recommendations play a significant role in the achievement of maximum safeguards and security objects in the most cost-effective manner. The incumbent recognizes problems at the earliest possible stage before security damage has occurred and/or when addressing vulnerabilities will not entail inordinate expenditures.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 7 of 8 ✓ Critical ___ Noncritical

Maintains systems of internal controls for the office that are consistent with DOE guidelines and objectives.

PERFORMANCE STANDARDS

MARGINAL

Same as Fully Successful except that incumbent must be reminded of the importance of internal control procedures such that evaluation takes place as required. The development of corrective actions, over matters which incumbent has control, occasionally requires upper management assistance.

FULLY SUCCESSFUL

Remains abreast of DOE guidelines and directives, evaluates internal control procedures at appropriate intervals or designated time, and takes prompt corrective actions as necessary.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

Effectively and aggressively maintains systems of internal control, consistent with DOE guidelines and directives, which reflects sound understanding of program requirements, creative application of controls or procedures, and daily adherence to adopted methodologies to achieve desired program results. Program successes are directly attributable to incumbent's ingenuity and support.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 8 of 8 ✓ Critical ___ Noncritical

Represents DOE Safeguards and Security interests at all levels within Headquarters, field offices, contractors, as well as with other Departments, agencies and the private sector.

PERFORMANCE STANDARDS

MARGINAL

Generally able to interface effectively with contacts. Responds to inquiries by other offices and activities in a positive manner. Due to a lack of knowledge, communication skills, assertiveness or judgment, assistance by the supervisor is sometimes needed to effectively bring about desired results. Overall performance is acceptable, but occasionally marred by significant shortcomings which reflect adversely upon the organization or detract from mission accomplishment.

FULLY SUCCESSFUL

Maintains poise and effectiveness under pressure and unusual circumstances. Consistently fosters a high degree of cooperation in personal and branch work relationships; expresses ideas clearly and concisely in face-to-face situations, as well as in written communication. Provides logical and concise presentations of facts and rationale which are persuasive and normally successful. Conveys a positive professional image, both personally and as a representative of the Office of Safeguards and Security.

OUTSTANDING ___ Generic standard will be used. X Generic standard will not be used

Demonstrates exceptional poise, communication skills, job knowledge and judgment in all aspects of dealing with individuals and organizations. Provides unusually effective representation of the Office of Safeguards and Security interests. Excels when confronted with difficult situations and tasks.

PMRS/PMS PERFORMANCE RATING

NAME Richard J. Levernier SOCIAL SECURITY NUMBER 350-42-1453

Item I. INSTRUCTIONS.

1. Indicate the title of each element from the Performance Appraisal Plan, DOE 3430.7; and indicate whether it is critical (C) or noncritical (NC). Assign a weight of 2 to each critical element and 1 to each noncritical element.
2. Rate each element by assigning a value for each element based on the following: Unacceptable = 0; Marginal = 1; Fully Successful = 2; Highly Successful = 3; Outstanding = 4. Document performance on the reverse side of this page when an element is rated Outstanding based on the generic standard.
3. Perform the computations indicated, and check the appropriate summary rating.

ELEMENT NUMBER (Title)	C NC	WT.	ELEMENT RATING U=0 M=1 F=2 HS=3 O=4	WEIGHTED RATING
1 ACCOUNTABILITY TO SENIOR MANAGEMENT	C	2 x	4	= 8
2 PLANS, ORGANIZES, DIRECTS, & CONTROLS TASKINGS	C	2 x	4	= 8
3 SETS PERFORMANCE STANDARDS/REVIEWS PERFORMANCE	C	2 x	4	= 8
4 PROVIDES EXPERT ADVICE AND GUIDANCE	C	2 x	4	= 8
5 KNOWLEDGE OF ANALYSIS & ASSESSMENT METHODOLOGIES	C	2 x		= 8
6 EVALUATES, SUPPORTS, & DEFINEDS IMPROVEMENT PROJECT	C	2 x		= 8
7 MAINTAINS SYSTEMS OF INTERNAL CONTROLS	C	2 x		= 8
8 REPRESENTS DOE's INTERESTS	C	2 x		= 8
9		x		=
10		x		=
TOTAL		16		64

$$\frac{64}{\text{TOTAL OF WEIGHTED RATING}} \div \frac{16}{\text{TOTAL OF WEIGHTS}} = \frac{4.0}{\text{SUMMARY RATING SCORE}}$$

SUMMARY RATING

U ____

M ____

FS ____

HS ____

O ✓

SUMMARY RATING LEVELS	CRITERIA
1. UNACCEPTABLE (U)	– One or more critical elements do not meet the "Marginal" standard regardless of total score
2. MARGINAL (M)	– Summary rating score of 1.9 or less and no critical element is rated below "Marginal" OR A score above 1.9, but one or more critical elements is rated "Marginal" (no critical element is rated below "Marginal")
3. FULLY SUCCESSFUL (FS)	– Summary rating score of 2.0 through 2.9 and no critical element is rated below "Fully Successful" OR A score above 2.9, but one or more noncritical elements is rated "Unacceptable" (no critical element is rated below "Fully Successful")
4. HIGHLY SUCCESSFUL (HS)	– Summary rating score of 3.0 through 3.7 and no critical element is rated below "Fully Successful" and no noncritical elements is rated below "Marginal" OR A score above 3.7, but one or more noncritical elements is rated "Marginal" (no noncritical element is rated below "Marginal" and no critical element is rated below "Fully Successful")
5. OUTSTANDING (O)	– Summary rating score of 3.8 or higher and no element is rated below "Fully Successful"

✓ Annual Rating of Record; ____ Detail; ____ Position Change; ____ Temporary Promotion

____ Other, specify:

Item II - CERTIFICATIONS

(Signature of Rating Official)	(Title & Organization)	(Date)
Edward J. McCallum	Director, NN-51	2/22/99
(Signature of Reviewing Official)	(Title & Organization)	(Date)
Joseph S. Mahaley	Director, NN-50	2/22/99

Employee - I have reviewed this performance rating, and it has been discussed with me. Check if appropriate:
_____ Comments are attached.

Richard J. Levernier

Richard J. Levernier
(Signature)

3-2-99
(Date)

Item III. DOCUMENTATION.
Describe actual performance in relation to the standard for each element that is rated "Outstanding" based on the generic Outstanding standards. (Attach a sheet of bond paper if more space is needed.)

JOINT STAFF INTEGRATED VULNERABILITY ASSESSMENT TEAM (JSIVA)

OSCS MALCOLM HILL
TERRORIST OPTIONS

MR WILLIAM PIPER
OPERATIONS READINESS

DR YOUNG SOHN
STRUCTURAL ENGINEER

CDR MIKE JOHNSON
JOINT STAFF

MR CARL FRANQUET
SECURITY OPERATIONS

SFC FRED STRUBER
SECURITY OPERATIONS

LCDR JOHN SOMMER
INFRASTRUCTURE

JACK DIBRELL
COL, USA
TEAM CHIEF

PRESENTED OCTOBER 1998 TO
MR RICHARD LEVERNIER
"IN RECOGNITION OF YOUR SUPPORT FOR DoD'S ANTITERRORISM/FORCE PROTECTION PROGRAM

DOE F 3430.7 (4-86)
(All Previous Editions are Obsolete)

DEPARTMENT OF ENERGY

1998

PERFORMANCE RECORD

FOR

PERFORMANCE MANAGEMENT AND RECOGNITION SYSTEM EMPLOYEES

AND

PERFORMANCE MANAGEMENT SYSTEM EMPLOYEES

NAME OF EMPLOYEE RICHARD J. LEVERNIER

SOCIAL SECURITY NUMBER 350-42-1453

POSITION TITLE/PAY PLAN/SERIES/GRADE SECURITY SPECIALIST, GS-080-15

ORGANIZATION & LOCATION ASSESSMENT AND INTEGRATION STAFF, NN-513

DOE F 3430.7 (4-86)
(All Previous Editions Are Obsolete)

U.S. Department of Energy

CERTIFICATIONS

Section A CERTIFICATION OF DISCUSSION & ISSUANCE OF ELEMENTS/STANDARDS

a. I have received a copy of my elements/standards for this appraisal period and have been provided an opportunity to discuss them with the rating official. (Employee may provide comments on the reverse side of this form).

CHECK IF APPLICABLE

b. ____ The elements/standards used in the Performance Appraisal Plan for the previous annual rating period will remain in effect during this rating period, which begins 01/01/97 and ends 12/31/97

Richard J. Levernier — *(Signature of Employee)* — MARCH 20, 1997 *(Date)*

Brooks E. Todd, Acting Director, NN-513 — *(Signature of Rating Official)* — 3/21/97 *(Date)*

Edward S. McCallum, Director, NN-51 — *(Signature of Reviewing Official)* — 3/24/97 *(Date)*

Section B CERTIFICATION OF PROGRESS REVIEW

Performance and progress to date have been discussed with the employee in accordance with DOE 3430.3A.

Richard J. Levernier — *(Signature of Employee)* — JUNE 20, 1997 *(Date)*

Brooks E. Todd — *(Signature of Rating Official)* — 6/20/97 *(Date)*

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial) 2. Pay Plan/Series Grade 3. Rating Period

LEVERNIER, RICHARD J. GS-080-15 From:
To:

4. Check One:
_X_ Annual Rating of Record ___ Detail ___ Position Change ___ Temporary Promotion
___ Other, specify:

PERFORMANCE ELEMENT Number 1 of 8 ____Critical ____Noncritical

Accountability to senior management of the Office of Safeguards and Security (OSS), Office of Security Affairs, and the Department of Energy (DOE).

PERFORMANCE STANDARDS

MARGINAL
Lacks understanding of the needs of senior management. Informs top management of routine problems arising out of the day-to-day activities and consults management concerning proposed routine actions. Normally responsive to management directions and requests. Usually informs management of significant events or occurrences in a timely fashion, but sometimes fails to do so. Occasionally fails to provide adequate support to senior management's programs or priorities as evidenced by failure to convey information or supporting rationale to subordinates, contractors, or other individuals. Sometimes the incumbent's failure to abide by established priorities detracts from program success.

FULLY SUCCESSFUL
Advises management of significant occurrences or developments and trends indicating potential for serious problems. Anticipates senior management's needs. Reporting is timely and objective. Routinely responsive to management directions, requests, and needs. Proposes reasonable solutions or alternatives to prevent or minimize negative consequences. Demonstrates loyalty and team spirit in actions taken and performance of duties.

OUTSTANDING ___ Generic Standard will be used. _X_ Generic standard will not be used.
Recognized as an exceptionally competent professional; consistently responsive to management directions, requests, and needs. Highly adept at discerning what information senior management requires to perform effectively, and at providing pertinent information in a succinct form and timely fashion. Unfailing in providing strong support to senior management positions. Effectively demonstrates personal loyalty and fosters team spirit among fellow workers and subordinates.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 2 of 8 ____Critical ____Noncritical

Plans, organizes, directs, and controls staff taskings and work efforts related to DOE safeguards and security assessment and integration issues.

PERFORMANCE STANDARDS

MARGINAL

Assigned tasks are usually monitored to completion and generally meet guidance regarding scope, reporting, timeliness and other specified conditions. Occasional supervisory involvement is required to ensure completion of priority action items. Work products must be reviewed thoroughly by supervisor to ensure consistent adherence to quality standards. Approaches to management tasks sometimes indicate inadequate planning or organization. Occasionally incumbent must be reminded to manage or apply allocated funding or other resources judiciously. Incumbent sometimes fails to coordinate resource requirements adequately, balance workloads or provide clear direction to team members or contractors where appropriate.

FULLY SUCCESSFUL

Incumbent effectively plans and assigns work associated with taskings. Coordinates resource requirements as appropriate. Sets priorities and establishes schedules for work completion. Ensures timely performance of work, makes changes in work assignments to balance work loads and meet schedules. Priority action items and taskings are complete on time or corrective action is taken at appropriate times. Work products reflect creative thought, thorough research and analysis of issues and problems, attention to detail, and adherence to standards, as appropriate. Allocated funds and other resources are effectively applied to meaningful tasks and are professionally managed.

OUTSTANDING ___Generic standard **will** be used. _X_Generic standard **will not** be used

Incumbent displays superior initiative in identifying and addressing substantive issues and problems not assigned by supervisor. Work efforts are consistently planned and executed to provide orderly flow of high quality products to fulfill tasking and enhance the safeguards and security program. Exceptional leadership results in a sustained high degree of staff productivity. Incumbent's grasp of responsibilities and actions taken clearly reflect exceptional competence and demonstrated ability to assume more demanding responsibilities.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial) — 2. Pay Plan/Series Grade

LEVERNIER, RICHARD J. — GS-080-15

PERFORMANCE ELEMENT Number 3 of 8 ____Critical ____Noncritical

Sets performance standards and reviews the performance of team members.

PERFORMANCE STANDARDS

MARGINAL

Higher level of management involvement is sometimes required to resolve day-to-day team member problems. Meets periodically or upon request with assigned personnel to discuss and establish priorities and performance expectations. Communicates OSS management policies and initiatives. Training and developmental needs of team members are discussed. Evaluates team members' performance. Performance of duties is generally adequate but incumbent sometimes fails to establish priorities, convey information or provide necessary guidance to subordinates thereby contributing to morale problems.

FULLY SUCCESSFUL

Informally appraises team members' performance at least quarterly and accomplishes formal appraisals as required. Team members' career goals are discussed and individual developmental needs are discussed and accommodated within government interests, budgetary constraints and scheduling considerations. Ensures recognition of exceptional work by team members and initiates appropriate action to address performance problems.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

In addition to Fully Successful, consistently achieves exceptional success in motivating team members to strive for excellence in the accomplishment of their duties. Identifies team personnel who evidence promising developmental potential and seek assignments which will benefit both the individuals and the organization and makes recommendations to Division Director. Incumbent continually strives to improve the productivity of individuals within the team; displays creativity and initiative in devising and recommending motivational programs.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 4 of 8 ____Critical ____Noncritical

Provides expert advice and planning guidance on the development, review, and analysis of facility Master Safeguards and Security Agreements (MSSAs) that cover safeguards and security protection of operations at nuclear weapons design laboratories, nuclear material weapons and production facilities, and nuclear weapons testing installation.

PERFORMANCE STANDARDS

MARGINAL

The incumbent sometimes fails to adequate advice and assistance to field offices in the integration of MSSAs into the protection programs at the specific sites. May show insufficient knowledge of DOE and other Government regulations and directives pertaining to safeguards and security as evidenced by recommendations that do not fully address critical issues and/or site-specific considerations.

FULLY SUCCESSFUL

Consistently furnishes expert advice and planning guidance on the development, review, and analysis of facility MSSAs. The incumbent functions as a focal point for integration activities to establish formal MSSAs between Headquarters and field office managers on protection programs at each DOE site based upon site-specific considerations.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

The incumbent provides unusually positive and effective leadership in the formulation and implementation of MSSAs for DOE nuclear weapons facilities that are fully compatible with DOE and other Governmental regulations pertaining to safeguards and security at facilities critical from the standpoint of national security. Advice and guidance is regularly recognized as authoritative and is readily accepted due to the technical soundness of recommendations and advice.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 5 of 8 ____Critical ____Noncritical

Maintains comprehensive knowledge of analysis and assessment methodologies and techniques. Ensures exploitation of new techniques and technologies that contribute to mission accomplishment in effective ways.

PERFORMANCE STANDARDS

MARGINAL

The incumbent occasionally shows limited knowledge of state-of-the-art safeguards and security concepts and technology. Shows reluctance to take action to ensure the integration of new techniques and technologies that could enhance achievement of mission objectives. The incumbent may not adequately present to senior management the need for and the benefits of incorporating new safeguards and security technologies into protection programs for field operations.

FULLY SUCCESSFUL

The incumbent effectively ensures the exploitation of new techniques and technologies that contribute to mission accomplishment. Applies knowledge of state-of-the-art safeguards and security concepts and technologies in reviewing and recommending adjustments to protection programs for DOE operations offices and cognizant facilities. The incumbent generally presents sound and convincing cases to senior management regarding the need for and the benefits of using new safeguards and security technologies.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

Recommendations regarding the integration of new safeguards and security concepts and technologies into field operations protection program are nearly always accepted by senior management because of the incumbent's stature as a widely-recognized authority in the discipline. The incumbent regularly shows how new methods would enhance safeguards and security objectives at a cost savings to the Government.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 6 of 8 ____Critical ____Noncritical

Evaluates, supports, and defends safeguards and security improvement projects throughout the planning and budget cycles. Provides a focal point within DOE to ensure prioritization of safeguards and security projects and activities.

PERFORMANCE STANDARDS

MARGINAL

The incumbent provides superficial assessments of safeguards and security vulnerabilities and deficiencies that, in some cases, detract from efforts to assign appropriate priorities and resources to address such problems. May not recognize how cost saving may be achieved through safeguards and security standardization at some DOE sites. The incumbent sometimes does not effectively coordinate safeguards and security projects and improvement activities with other DOE elements. May not consistently monitor the status of safeguards and security implementation and improvement activities.

FULLY SUCCESSFUL

The incumbent is conscientious in overseeing the status of safeguards and security implementation and improvement activities. Coordinates projects and improvement endeavors with other DOE elements. Efforts contribute to valid identification of safeguards and security vulnerabilities and deficiencies and that such problems receive requisite attention and commitment of resources.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

The incumbent's evaluations of safeguards and security vulnerabilities and deficiencies are consistently thorough and materially contribute to the assignment of appropriate prioritization and resource commitments through the planning and budget cycles, resulting in substantial improvement in protection programs. Maintains stature as an expert in safeguards and security implementation and improvement activities, and is recognized by other DOE elements as an authority whose coordination efforts, assessments, and recommendations play a significant role in the achievement of maximum safeguards and security objects in the most cost-effective manner. The incumbent recognizes problems at the earliest possible stage before security damage has occurred and/or when addressing vulnerabilities will not entail inordinate expenditures.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 7 of 8 ____Critical ____Noncritical

Maintains systems of internal controls for the office that are consistent with DOE guidelines and objectives.

PERFORMANCE STANDARDS

MARGINAL

Same as Fully Successful except that incumbent must be reminded of the importance of internal control procedures such that evaluation takes place as required. The development of corrective actions, over matters which incumbent has control, occasionally requires upper management assistance.

FULLY SUCCESSFUL

Remains abreast of DOE guidelines and directives, evaluates internal control procedures at appropriate intervals or designated time, and takes prompt corrective actions as necessary.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

Effectively and aggressively maintains systems of internal control, consistent with DOE guidelines and directives, which reflects sound understanding of program requirements, creative application of controls or procedures, and daily adherence to adopted methodologies to achieve desired program results. Program successes are directly attributable to incumbent's ingenuity and support.

PERFORMANCE APPRAISAL PLAN

1. Name (Last, First, Middle Initial)
LEVERNIER, RICHARD J.

2. Pay Plan/Series Grade
GS-080-15

PERFORMANCE ELEMENT Number 8 of 8 ____Critical ____Noncritical

Represents DOE Safeguards and Security interests at all levels within Headquarters, field offices, contractors, as well as with other Departments, agencies and the private sector.

PERFORMANCE STANDARDS

MARGINAL

Generally able to interface effectively with contacts. Responds to inquiries by other offices and activities in a positive manner. Due to a lack of knowledge, communication skills, assertiveness or judgment, assistance by the supervisor is sometimes needed to effectively bring about desired results. Overall performance is acceptable, but occasionally marred by significant shortcomings which reflect adversely upon the organization or detract from mission accomplishment.

FULLY SUCCESSFUL

Maintains poise and effectiveness under pressure and unusual circumstances. Consistently fosters a high degree of cooperation in personal and branch work relationships; expresses ideas clearly and concisely in face-to-face situations, as well as in written communication. Provides logical and concise presentations of facts and rationale which are persuasive and normally successful. Conveys a positive professional image, both personally and as a representative of the Office of Safeguards and Security.

OUTSTANDING ___Generic standard will be used. _X_Generic standard will not be used

Demonstrates exceptional poise, communication skills, job knowledge and judgment in all aspects of dealing with individuals and organizations. Provides unusually effective representation of the Office of Safeguards and Security interests. Excels when confronted with difficult situations and tasks.

(All Previous Editions Are Obsolete)

U.S. Department of Energy

PMRS/PMS PERFORMANCE RATING

NAME Richard J. Levernier SOCIAL SECURITY NUMBER 350-42-1453

I. INSTRUCTIONS.

1. Indicate the title of each element from the Performance Appraisal Plan, DOE 3430.7; and indicate whether it is critical (C) or noncritical (NC). Assign a weight of 2 to each critical element and 1 to each noncritical element.
2. Rate each element by assigning a value for each element based on the following: Unacceptable = 0; Marginal = 1; Fully Successful = 2; Highly Successful = 3; Outstanding = 4. Document performance on the reverse side of this page when an element is rated Outstanding based on the generic standard.
3. Perform the computations indicated, and check the appropriate summary rating.

ELEMENT NUMBER	(Title)	C NC	WT.	ELEMENT RATING U=0	M=1	F=2	HS=3	O=4	WEIGHTED RATING
1	ACCOUNTABILITY TO SENIOR MANAGEMENT	C	2 X					4 =	8
2	PLANS, ORGANIZES, DIRECTS, & CONTROLS TASKINGS	C	2 X					4 =	8
3	SETS PERFORMANCE STANDARDS/REVIEWS PERFORMANCE	C	2 X					4 =	8
4	PROVIDES EXPERT ADVICE AND GUIDANCE	C	2 X					4 =	8
5	KNOWLEDGE OF ANALYSIS & ASSESSMENT METHODOLOGIES	C	2 X					4 =	8
6	EVALUATES, SUPPORTS, & DEFNEDS IMPROVEMENT PROJECT	C	2 X					4 =	8
7	MAINTAINS SYSTEMS OF INTERNAL CONTROLS	C	2 X					4 =	8
8	REPRESENTS DOE's INTERESTS	C	2 X				3	=	6
9			X					=	
10			X					=	
	TOTAL		16						62

$$\frac{62}{\text{TOTAL OF WEIGHTED RATING}} \div \frac{16}{\text{TOTAL OF WEIGHTS}} = \frac{3.9}{\text{SUMMARY RATING SCORE}}$$

SUMMARY RATING

U _____

M _____

FS _____

HS _____

O ✓

SUMMARY RATING LEVELS	CRITERIA
1. UNACCEPTABLE (U)	– One or more critical elements do not meet the "Marginal" standard regardless of total score
2. MARGINAL (M)	– Summary rating score of 1.9 or less and no critical element is rated below "Marginal" OR A score above 1.9, but one or more critical elements is rated "Marginal" (no critical element is rated below "Marginal")
3. FULLY SUCCESSFUL (FS)	– Summary rating score of 2.0 through 2.9 and no critical element is rated below "Fully Successful" OR A score above 2.9, but one or more noncritical elements is rated "Unacceptable" (no critical element is rated below "Fully Successful")
4. HIGHLY SUCCESSFUL (HS)	– Summary rating score of 3.0 through 3.7 and no critical element is rated below "Fully Successful" and no noncritical elements is rated below "Marginal" OR A score above 3.7, but one or more noncritical elements is rated "Marginal" (no noncritical element is rated below "Marginal" and no critical element is rated below "Fully Successful")
OUTSTANDING (O)	– Summary rating score of 3.8 or higher and no element is rated below "Fully Successful"

_____ Annual Rating of Record; _____ Detail; _____ Position Change; _____ Temporary Promotion

_____ Other, specify:

Item II – CERTIFICATIONS

(Signature of Rating Official) — (Title & Organization) — (Date)

Brooks Todd — Acting Director, NN-513 — 2/2/98.

(Signature of Reviewing Official) — (Title & Organization) — (Date)

Edward J. McCallum — Director, NN-51 — 2/2/98

Employee – I have reviewed this performance rating, and it has been discussed with me. Check if appropriate:

_____ Comments are attached.

Richard J Levernier — 2-2-98

Richard J Levernier (Signature) — (Date)

Item III. DOCUMENTATION.
Describe actual performance in relation to the standard for each element that is rated "Outstanding" based on the generic Outstanding standard. (Attach a sheet of bond paper if more space is needed.)

• U.S.GPO:1986-0-621-651/00092

Department of Energy
Office of Civilian Radioactive Waste Management
Yucca Mountain Site Characterization Office
P.O. Box 98608
Las Vegas, NV 89193-8608

APR 20 1995

Gail M. Pesyna, Deputy Assistant Secretary for Management and Finance, Environmental Management, HQ (EM-10) FORS

CONTINUED SAFEGUARDS AND SECURITY (S&S) MANAGEMENT AND TECHNICAL ASSISTANCE - RICHARD LEVERNIER (SCPB: N/A)

The purpose of this letter is to request continued professional assistance from Richard Levernier, who will soon transfer to your organization (EM-15). As you may be aware, Mr. Levernier, at the request of the Project Manager, Yucca Mountain Site Characterization Project (YMP), has provided support to the Yucca Mountain Site Characterization Office (YMSCO) in developing an overall S&S program for the YMP. This support has proven to be invaluable in terms of formulating the YMSCO S&S program. As the S&S program progresses, it is clear that maintaining continuity in our management approach to program development is crucial. Additionally, because of the unique nature of the YMSCO S&S program, its high visibility, and the fact that it is the only U.S. Department of Energy facility to receive licensing from the U.S. Nuclear Regulatory Commission, the project provides especially challenging S&S issues.

Since July of 1994, Mr. Levernier has been very successful in identifying and developing the necessary S&S program elements. Because of his efforts, YMSCO is currently in the process of recruiting and training S&S professionals that will ultimately manage the S&S program. However, there remain many near-term critical initiatives that face YMSCO which will require the expertise of a senior S&S manager. Therefore, the most appropriate method for accomplishing these initiatives and ensuring program continuity is to request continued support from Mr. Levernier at a 20 percent level for the remainder of the current calendar year. During this period, Mr. Levernier's duties will consist of monitoring the progress of S&S program development by providing guidance, amplification, and contractor direction in overall security program development. As has been the case in the past, funding for travel associated with this effort will be provided by YMSCO.

Additionally, it is my understanding that Mr. Levernier's future supervisor, Louis Ritchie, has tentatively agreed to this type and level of support. Please give this request your consideration and contact me at (702) 794-7586, at your earliest possible convenience.

J. Russell Dyer
Deputy Project Manager

DPM:JRD-2267

YMP-5

cc:
L. H. Barrett, HQ (RW-2) FORS
C. M. Lukasik, HQ (RW-16) FORS
Samuel Rousso, HQ (RW-40) FORS
L. C. Ritchie, HQ (EM-15) CXXI
R. J. Levernier, HQ (EM-15) CXXI
H. C. White, Jr., YMSCO, NV
S. L. Rouse, YMSCO, NV

United States
Department of Energy

Monetary Award for Superior Job Performance

Presented to

Richard J. Levernier

In recognition of

your outstanding performance which has contributed significantly to the mission of the Department of Energy, and is, therefore, deserving of this special commendation.

Mark Silverman, Manager

January 6, 1995
Date

United States
Department of Energy

Outstanding Performance Appraisal

Granted to

Richard Levernier

In recognition of outstanding performance which has significantly contributed to the mission of the Department of Energy.

Robert M Weisman Jr Nov 12, 1992

Date

Department of Energy

ROCKY FLATS OFFICE
P.O. BOX 928
GOLDEN, COLORADO 80402-0928

April 26, 1992

Richard J. Levernier
U. S. Department of Energy
P. O. Box 928
Golden, Colorado 80040

Dear Rich,

As I am sure you are by now aware, I will soon be leaving my "temporary" detail at Rocky Flats and returning to my position as the Deputy Manager of the Nevada Field Office. I make this move with very mixed emotions as I have enjoyed managing the Rocky Flats Office.

It is rare that a manager has the opportunity to assemble a staff as I have. That fact in and of itself makes my decision to leave very difficult. I am extremely proud of this organization and the tremendous professionalism and talent it exudes. I believe this office will set the standard for DOE in terms of technical capability and professional commitment in the future.

The past two years could have been tremendously difficult for me as the day to day issues confronting Rocky Flats have not been easy nor has a lasting separation from my family and community.

The RFO staff has made this assignment a tremendous experience. I enjoyed working with this staff and feel privileged to have been a part of the Rocky Flats family.

Thank you for your personal commitment to Rocky Flats and to me.

Sincerely,

Bob

Robert M. Nelson, Jr.
Manager

Rich,
You have been a key to the success of Security improvements at Rocky Flats. I really appreciate all of your help to me and, your dedication to doing what is

EG&G ROCKY FLATS

EG&G ROCKY FLATS, INC.
ROCKY FLATS PLANT, P.O. BOX 464, GOLDEN, COLORADO 80402-0464 • (303) 966-7000

June 29, 1992

92-RF-7128

Mr. Richard Levernier
Security
DOE, RFO

ENERGY SECRETARY JAMES WATKINS VISIT, JUNE 12, 1992 - JOZ-441-92

Dear Mr. Levernier:

When Energy Secretary James Watkins decided to come to Rocky Flats, he kicked into motion a tremendous planning and operational effort that culminated in a successful visit June 12. As a contractor to the Department of Energy, we were proud to be a part of this effort.

This event could not have been pulled off by one person or one group. It took teamwork across plantsite and the willingness and determination to find ways to accomplish those tasks that had to be done both prior to his visit and during his stay here.

The result was not only a worthwhile experience for Secretary Watkins but provided us an opportunity to give all employees a long overdue 'thanks for a job well done.'

It was through efforts like yours, your cooperation and your support, that made it possible for us to do this.

The event marked employees' professionalism, pride and patriotism and their dedication to creating a new approach to business. You exemplified that through your efforts. Thank you.

Sincerely,

J.O. Zane
General Manager

MCK:jed

Department of Energy

ROCKY FLATS OFFICE
P.O. BOX 928
GOLDEN, COLORADO 80402-0928

JUN 10 1991

Richard Levernier Director
Safeguards & Security Division
Rocky Flats Office

OPA:91:4271

Dear Mr. Levernier:

One of the most important parts of our efforts to resume normal operations at Rocky Flats is to re-establish public credibility in the plant and in the people who work here. I believe that our press tour of May 9 went a long way toward helping the public understand that very professional people who know their jobs and are proud of what they do have and will continue to make Rocky Flats a safe place and a good place to work. All of the members of the team that made this tour a reality did a superb job of showing what we can do. I was extremely proud of everyone involved.

Please accept my thanks for helping with this effort. I know that it was difficult and an added burden to an already full agenda of urgent things, but it came off well and I truly believe we are making real progress. Again thank you for your extra effort to make this tour such a success.

Sincerely,

Robert M. Nelson, Jr.
Manager

EG&G ROCKY FLATS

EG&G ROCKY FLATS, INC.
ROCKY FLATS PLANT, P.O. BOX 464, GOLDEN, COLORADO 80402-0464 • (303) 966-7000

May 21, 1991

Rich Levernier
Safeguards & Security

BUILDING 559 MEDIA TOUR - THURSDAY, MAY 9, 1991 - JOZ-262-91

I want to express my personal appreciation to you for your extra effort in contributing to the May 9 media tour of Building 559. Your professionalism and conscientious support were crucial to the successful conclusion of the tour.

All participants on the tour team and the supporting players performed in an extraordinary manner. I cannot overemphasize the importance of opportunities such as this to help the media, and the public, understand our operations and the focus we place on safety, security, and environmental protection.

I realize the scheduling of this tour placed additional burdens on your resources, and that many of you had to make sacrifices to satisfy the tour requirements. I appreciate this type of extra effort.

Please thank all the people that joined in helping you make the media tour a success for all involved.

J. O. Zane

United States
Department of Energy - Rocky Flats Office

Outstanding Performance Appraisal

Granted to

Richard J. Levernier

In recognition of outstanding performance which has significantly contributed to the mission of the Department of Energy.

Robert M Nelson

April 8, 1992
Date

DOE F3430.6 (10/90)

This Certificate is Presented to

Rich Levernier

for improving the Credibility to our

Security Program for the Rocky Flats Plant

APR 0 9 1992

Date

Robert M Nelson

Robert M. Nelson, Jr.
Manager, Rocky Flats Office

LITHO IN U.S.A.

United States
Department of Energy

Monetary Award for Superior Job Performance

Presented to

Richard J. Levernier

In recognition of your outstanding job performance. Your knowledge, application of professional skills, and managerial effectiveness have contributed significantly to the achievement of Defense Program goals and objectives.

Troy E. Wade II
Acting Assistant Secretary for Defense Programs

12/8/88
Date

United States
Department of Energy

Monetary Award for Superior Job Performance

Presented to

Richard J. Levernier

In recognition of your exceptional job performance in Defense Programs. Your professional competence, level of technical skills, and attention to responsibilities were instrumental in achieving program goals and objectives.

Troy E. Wade II
Acting Assistant Secretary for Defense Programs

Date December 1987

DOE F 3460.8 (3-85)

United States
Department of Energy

Certificate of Appreciation

Presented to

Richard Levernier

For your dedicated and expert assistance in the development of the Department of Energy's Safeguards and Security Standards and Criteria.

S. R. Foley, Jr.
Assistant Secretary for Defense Programs

6/96

Department of Energy
Washington, D.C. 20585

February 4, 1985

MEMORANDUM FOR Richard J. Levernier

SUBJECT: Letter of Appreciation

I would like to take this opportunity to express my sincere appreciation to you for your valuable contribution during the Inspection and Evaluation Division's inspection of the Department of Energy Headquarters facilities, January 22 through February 1, 1985.

The success of this inspection will assure a more effective protection program of Department of Energy Headquarters and will help ensure adequate security for the personnel and facilities at the Forrestal and Germantown locations.

William W. Hoover
Assistant Secretary
for Defense Programs

The State of South Carolina

By His Excellency

THE GOVERNOR AND COMMANDER-IN-CHIEF IN AND OVER THE STATE AFORESAID

TO Richard J. Levernier, P.O. Box A, Aiken, S.C.

KNOW ALL MEN BY THESE PRESENTS:

By virtue of authority vested in me as Governor in and over the State aforesaid, I, reposing special trust and confidence in your ability, care, prudence and integrity, have constituted appointed and hereby Commission you, the said Richard J. Levernier Special State Constable(DOE) in the State aforesaid, to have, hold, exercise and enjoy the said office of Special State Constable(DOE) and to enforce the Laws of the State aforesaid, serving without compensation from the State.

This Commission is to continue in force until January 27, 1986.

GIVEN UNDER MY HAND and the Seal of the State, in Columbia this 7th day of June in the year of our Lord one thousand nine hundred and 84 and the ~~one hundred and~~ 208th year of the Independence of the United States of America.

Richard W. Riley
GOVERNOR

John T. Campbell
SECRETARY OF STATE

APPRAISAL IS TO BE COMPLETED AT THE END OF APPRAISAL PERIOD.

DOE F 3430.8
(6-80)

U.S. DEPARTMENT OF ENERGY

PERFORMANCE APPRAISAL

(See Reverse for Instructions and Privacy Act Statement)

1. NAME OF EMPLOYEE: (First, Initial, Last)	2. SOCIAL SECURITY NO:	3. APPRAISAL PERIOD: ☐ Detail
Richard J. Levernier	350-42-1453	7/02/83-7/01/84 ☐ Temp. Promotic
ITLE AND POSITION NO.	**5. ORGANIZATION:**	**6. SERIES/GRADE:**
Chief, Personnel Security Branch	S&S Division	☐ Merit Pay GM-13

7. ELEMENT NO.	8. RATING CODE					9. DOCUMENTATION
	U	A	F	H	O	
1.					X	Mr. Levernier has identified and prioritized in an outstanding manner, the tasks and responsibilities of SR's Personnel Security Program. His knowledge of the deta and procedures which are required to properly fulfill mission of personnel clearance is outstanding and has drawn praise from Headquarter's OSS and S.R. O.G.C. Despite limited resources, the production rate of the Branch has improved due to Mr. Levernier's organizatio talents.
2.					X	Mr. Levernier has developed several internal managemen tools to assure that all Branch responsibilities are being fully addressed and met. Milestones are met in consistent manner and the products are comprehensive. His Branch personnel are well aware of the priorities objectives of the organization.
3.					X	Mr. Levernier is judged to be an outstanding supervisc who keeps his employees informed. He has made great strides in improving performance in the Branch through better definition of roles and responsibilities. He continuously strives to identify techniques to motivat personnel. Work performance, productivity, and overal efficiency have improved markedly under his guidance a leadership.
4.			X			
5.			X			
6.					X	Mr. Levernier has strived to meet all identified goals in an outstanding manner. His prioritization, trackin and implementation of the WSI PSQ program, enabled the Secretary of Energy's milestone to be met. Without hi contribution during the WSI transition period, the dat for facility acceptance would not have been met.
7.			X			
8.			X			

10. OVERALL APPRAISAL LEVEL:	11. RATER: (Signature) George P. Miserendino	14. GRADE GM-15
a. U ☐ c. F ☐ e. O ☒	12. TITLE: Director	15. DATE 7-10-84
b. A ☐ d. H ☐	13. ORGANIZATION: Safeguards & Security Division	

16. REVIEWER: (Signature) Charles E. Fox Jr.	20. EMPLOYEE: I have reviewed this performance appraisal and it has been discussed with me. ☐ Comments attached.
17. TITLE: Assistant Manager for Project Management	Richard J. Levernier 7.3.84
18. ORGANIZATION:	19. DATE: 7/10/84

NAME: Richard J. Levernier

POSITION AND GRADE: Chief, Personnel Security Branch, GM-13
Supervisory Personnel Security Specialist

I. Serves as first-line supervisor for the Personnel Security Branch. Develops, implements, and administers policies and procedures pertaining to access authorization and personnel clearance functions, foreign travel and alien and visitor control activities. Administers program involving cleared individuals hospitalized or otherwise treated for alcohol or mental illness. Establishes and maintains security awareness and security education programs. Administers division Privacy Act activities, classified document control and the visitor/badge program. Develops, implements and monitors the counter-intelligence program; monitors security infractions; maintains liaison with military and law enforcement organizations.

A. Specific Duties

1. Plans, executes, and supervises the SR personnel security programs, provides staff assistance and technical guidance to SR and directs contractor organizations in the development and control of their personnel security activities which consist of the following:

a. Develops and implements comprehensive policies and procedures for employees, consultants, and contractors involved in classified programs or projects.

b. Oversees the processing, granting, recording, and terminating of security clearances and access authorizations, including new cases, reinstatements, extensions and transfers.

c. Directs the review and analysis of individual requests for security clearance to assure that there is a need for the clearance in the performance of duties and that the required forms are properly completed for submission for appropriate investigations.

d. Directs the subsequent analysis of investigative reports and other pertinent data and grants clearances as appropriate.

e. Authorizes interviews with clearance applicants when the investigative record requires clarification, or additional information is necessary prior to determining their suitability for clearance.

f. Determines the need for initiating administrative review procedures and coordinates arrangements for Personnel Security Board Hearings including the selection of board members. Provides technical guidance to the board and furnishes necessary information to the subjects of the hearings and their counsels.

g. Determines need and arranges for psychiatric examination of applicants for clearance as well as for presently cleared personnel when information is received indicating the individual may be suffering from a mental illness which could potentially affect judgment or reliability.

h. Oversees the performance of compliance surveys and assessments, both on- and off-site.

2. Plans, executes, and directs the alien and visitor control functions which encompass SR and contractor organizations and consists of the following:

a. Development and/or implementation of policies and procedures for the control of visitors to SR classified facilities.

b. Review of proposed visits by aliens to facilities including the conduct of indices checks as appropriate.

c. Coordination of proposed travel to Soviet-bloc countries by cleared and formerly cleared individuals with DOE Headquarters when such individuals have had access to sensitive information. Approves all such travel when the individual has not had access to such information and current international circumstances do not indicate an unwarranted security risk. Conducts security briefings for travelers to Soviet-bloc countries.

3. Reviews security clearance files and investigative reports to determine the suitability of granting access to Top Secret information and crypto materials.

4. Continually monitors and appraises contractor performance to assure that the personnel security clearance function is carried out efficiently and effectively. Provides a formal evaluation of all major contractors involved in these functions which are used as the basis for award fee determinations.

5. Develops, implements and monitors the counter-intelligence program. Serves as the SR authority on intelligence operations, maintains appropriate liaison, and serves as point of contact with HQ and the intelligence community in interpreting information and requirements

6. Develops, implements and conducts the security awareness and security education programs. Establishes goals and objectives, conducts orientations and refreshers, and develops pertinent written materials.

7. Administers Privacy Act activities and responses for the division.

8. Administers classified document control activities for the division.

II. Aspects of Performance

A. Quality

Mr. Levernier has supervised and motivated his employees, Du Pont Operations and Construction, and WSI to improve the quality of all products in the personnel clearance program. This has been acknowledged by Headquarter's OSS on several occasions. The Administrative Review cases and hearing cases have improved in both success of adjudication and completeness. Visitor control procedures and processing have become more systematic, with improved policy changes initiated by Mr. Levernier.

B. Commitment

Mr. Levernier has displayed considerable initiative and creativity through the development of an in-branch tracking system for all personnel clearance cases. His improvements have enabled senior DOE management to have a greater appreciation for the mission and workload of the Branch. The new system has prioritized cases, highlighted problem areas, and facilitated the rapid processing of routine "clear" cases.

C. Adaptability

Mr. Levernier has greatly improved in this area during the past ten months. He has gained a good sense of direction and priorities from DOE senior management. An example is the emphasis placed on WSI and Du Pont construction employee clearance cases.

Mr. Levernier coordinated the recently conducted Southeast Inter-Agency Intelligence Conference despite the press of personnel security work. The conference was judged by all attendees to be a success.

III. E.E.O. Evaluation

Mr. Levernier, as the Chief, Personnel Security Branch, has had input on all personnel selections within the Branch. He is cognizant of the field offices program, goals and objectives and exercises appropriate input on the: selection and promotion, treatment, training and upward mobility, recognition, and discipline of personnel.

United States
Department of Energy

Cash Award for Special Act or Service

Presented to

Richard J. Levernier

In recognition of

exemplary performance of duties as Personnel Security Specialist, Safeguards and Security Division, during the period January 1981 to January 1983. His dedication and devotion to duty reflect great credit upon himself, the Chicago Operations Office, and the Department of Energy.

Robert H. Bauer

Robert H. Bauer
Manager

3/29/83

Date

United States Department of Agriculture

Certificate of Merit

awarded to

RICHARD J. LEVERNIER

FOR EXHIBITING CONSIDERABLE SKILL, FLEXIBILITY AND RESOURCEFULNESS DURING AN UNDERCOVER SURVEILLANCE OPERATION INVOLVING NATIONWIDE FOOD STAMP TRAFFICKING.

Margaret Sahs

ACTING INSPECTOR GENERAL

MAY 1980

AD-69 (1-72)

3

U.S. DEPARTMENT OF ENERGY
HEADQUARTERS

Performance Plan and Performance Appraisal Form
For
Performance Management System Employees

****

Employee **Richard Levernier** **Social Security** 350-42-1453

Position Title/Pay Plan/Series/Grade: Program Analyst, GS/343/15

Organization and Office of Foreign Visits & Assignments, Washington, DC

PERFORMANCE **From:** 10-01-2000 **To:** 09-30-2001

CHECK ONE: **ANNUAL RATING OF RECORD**

ADVISORY **Detail** **Position Change**

Temporary **Other**

SPECIAL RATING OF RECORD BASED ON:

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 1 of 8 Weight: 2 Rating: 4 (1,2,3, or 4)

One sentence summary statement:

Serves as the Lead Program Official for responding to external customers, including the general public (FIA) and oversight authorities (e.g., GAO, IG, Congress).

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

2. Analyzes incoming request and determines appropriateness to SO-24 program.

3. When applicable, routes to appropriate official. Identifies and locates information responsive to the customer request in DOE, SO and SO-24 systems of records.

4. Evaluates the sensitivity of the requested information for release to the public consistent with DOE polices.

5. Prepares informational briefings for Oversight customers (GAO, etc.) concerning areas of expressed interest. These briefings are a critical means of ensuring that these customers are fully informed and understand the complete scope and complexity of SO-24 Programs.

6. Ensures that all DOE responses are in the proper context, often isolated information conveys a distorted perspective concerning an issue. Utilizing the requisite staff resources each response is prepared to communicate an accurate and balanced description of the requested item.

7. Provides all relevant information in order to ensure that DOE Programs are evaluated appropriately.

8. Prepare letters of transmittal to customers requesting information.

(NOTE: This page may be reproduced as necessary)

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 2 of 8 Weight: 2 Rating: 3 (1,2,3, or 4)

One sentence summary statement:

Serves as manager of SO's Official Foreign Travel Program

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Ensures that all SO Official Foreign Travel requests are processed in a timely manner consistent with DOE policy.

2. Provides SO senior management with periodic reports concerning the Official Foreign Travel Program budget and traveler compliance with requirements, e.g. trip reports.

3. Provides SO personnel advice and assistance concerning Official Foreign Travel.

4. Ensures that country clearance, including US Department of State approval, is obtained on a timely basis for all SO Official Foreign Travel.

5. Provides SO staff advice and assistance utilizing the Foreign Travel Management System (FTMS) database.

6. Develops appropriate documentation for incorporation of the Official Foreign Travel Program into SO-24's mission and function planning.

(NOTE: This page may be reproduced as necessary)

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 3 of 8 Weight: 2 Rating: 3 (1,2,3, or 4)

One sentence summary statement:

Serves as SO-24's representative to DOE's Sensitive Subjects Development and Implementation activities.

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Serves as the SO-24 Representative on the DOE Sensitive Subjects List (SSL) Technical Review Group.

2. Provides advise and assistance to SO staff concerning the SSL.

3. Ensures that SO personnel have a comprehensive awareness of sensitive subjects and that Foreign Interactions take into account this important aspect of security.

4. Ensures that the SO-24 Foreign Visits and Assignments database (FACTS) appropriately characterizes DOE sensitive subjects.

5. Coordinates with other DOE and Federal entities concerning sensitive subjects.

6. Ensures that the DOE Sensitive Subjects List is considered prior to release of information to the public.

(NOTE: This page may be reproduced as necessary)

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 4 of 8 Weight: 1 Rating: 4 (1,2,3, or 4)

One sentence summary statement:

Provides management guidance and supervision for professional staff involved in SO-24's Official Foreign Travel Operations.

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Develops draft recommendations for input to performance plans.

2. Evaluates performance and prepares input recommendations for detail and annual performance appraisals.

4. Recommends Employees for performance awards, and develops supporting documentation.

5. Develops recommendations for priorities and work plans.

6. Recommends and supports training/career development activities for Employees.

7. Mentors junior Employees, providing program training and guidance, and encouraging professional growth.

(NOTE: This page may be reproduced as necessary)

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 5 of 8 Weight: ~~1~~ 2 Rating: 4 (1,2,3, or 4)

One sentence summary statement:

Represent the Office and DOE in briefings, conferences and working groups with other DOE offices and/or federal agencies on problems, issues and activities involving foreign visits and assignments issues.

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Establish and maintain contacts with DOE program offices and field elements to facilitate communication in support of departmental goals.

2. Develop and deliver presentations at program conferences on subjects related to foreign visits and assignments policy and procedures.

3. Prepare and present briefings for program secretarial offices, DOE senior management, Congress, the Department of State, other federal agencies, and the IAEA on foreign visits and assignments related issues and activities.

4. Represent SO in working groups engaged in foreign visits and assignments planning to support DOE's mission.

5. Demonstrate success in influencing adoption of the SO-24 position.

6. Prepare issue papers and reports for use by the Department in response to inquiries from government oversight entities (i.e., GAO).

7. Prepare issue papers and reports for use by the Department in response to inquiries from non-government organizations and the public.

(NOTE: This page may be reproduced as necessary)

Employee Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 6 of 8 Weight: 2 Rating: 3 (1,2,3, or 4)

One sentence summary statement:

Serves as the DOE Official Foreign Travel Program Transition Team Manager.

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Develops and coordinates the DOE Official Foreign Travel Transition Plan.

8. Develops and coordinates the DOE Official Foreign Travel Transition Agreement

9. Develops and coordinates the DOE Official Foreign Travel Memorandum of Agreements.

10. Develops and coordinates the DOE Official Foreign Travel Program Assessment.

11. Develops and coordinates the DOE Official Foreign Travel Formal Program Acceptance memorandum.

12. Ensures that the new FTMS database is complimentary to other SO-24 Foreign Interactions information management systems.

13. Reviews GAO and IG reports for potential applicability in SO-24 official and unofficial travel programs.

(NOTE: This page may be reproduced as necessary)

Employee Name: Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 7 of 8 Weight: 2 Rating: 4 (1,2,3, or 4)

One sentence summary statement:

Performance is responsive to senior management of the Office of Foreign Visits and Assignments (SO-24), Office of Security Affairs (SO-20), Office of Security and Emergency Operations (SO), and the Department of Energy (DOE).

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Informs top management of routine problems arising out of the day-to-day activities and consults management concerning proposed routine actions.

2. In a timely manner, informs top management of significant occurrences or developments and trends indicating potential for serious problems.

3. Provides effective support to senior management's programs or priorities by conveying information or supporting rationale to subordinates, contractors, or other individuals.

4. Highly adept at discerning what information senior management requires to perform effectively, and at providing pertinent information in a succinct, objective, and timely fashion.

5. Proposes reasonable and effective solutions or alternatives to prevent or minimize negative consequences.

6. Contributing to the program's success by abiding by priorities established by management.

7. Effectively demonstrates loyalty to the program and fosters team spirit among fellow workers and team members.

(NOTE: This page may be reproduced as necessary)

Employee Name: Richard Levernier

PERFORMANCE APPRAISAL/MANAGEMENT PLAN

Performance Element: 8 of 8 Weight: 2 Rating: 4 (1,2,3, or 4)

One sentence summary statement:

Ensure effective support to all levels of stakeholders.

****

Tasks. Objectives and/or Activities Related to Element:
(Include relevant organizational goals, strategic plan objectives, related tasks.)

1. Provide SO-24's stakeholders with prompt, effective and courteous responses to issues and inquires.

2. Evaluate issues for relevancy to team mission, and redirect as appropriate.

3. Evaluate, determine and analyze current and future user community needs and develop recommendations for improvement.

4. Participates effectively in SO-24 Quality Committees.

5. Foster a cooperative alliance between Department of Energy (DOE) government and contractor employees to promote efficiency, excellence and organizational participation in the development of programmatic functions required for operational implementation of FV&A program and implementing systems support.

6. Identify problems, resolve issues and recommend solutions for areas within SO-24 program cognizance and/or area of purview.

7. Ensure appropriate documentation of issues and actions to resolve.

(NOTE: This page may be reproduced as necessary)

PERFORMANCE PLAN CERTIFICATIONS

Section A. Certification of Discussion & Issuance of Elements/Standards

Nevaire S. Rich *(Signed)* May 29, 2001

Nevaire S. Rich, Dep. Dir, SO-*24* *(Typed)*

Signature of Rating Official *Date*

Marshall O. Combs *(Signed)* May 29, 2001

Marshall O. Combs, Director, SO-24 *(Typed)*

Signature of Reviewing Official *Date*

Employee - I have reviewed and have been provided an opportunity to discuss my elements/standards for this period with the rating official.

Richard J. Levernier 5-30-01

Signature of Employee *Date*

__ *Employee refused to sign*

Section C. Certificate of Performance Rating:

Individual element		Weight:	Total:
Element 1.	4	2	8
Element 2.	3	2	6
Element 3.	3	2	6
Element 4.	4	1	4
Element 5.	4	2	8
Element 6.	3	2	6
Element 7.	4	2	8
Element 8.	4	2	8
Total weights:		15	Total 54

Overall Summary Rating (total points divided by total 3.6

Nevaire S. Rich (Signed)

Nevaire S. Rich, Dep. Dir., SO-24 (Typed)

Signature of Rating Official Date 11-8-01

Marshall O. Combs (Signed)

Marshall O. Combs, Dir. SO-24 (Typed)

Signature of Reviewing Official Date 11-8-01

Employee - I understand that my signature on the appraisal indicates only that I have reviewed the appraisal. I understand that failure to sign the appraisal does not affect its validity.

Richard J. Lorenzo NOV. 8, 2001

Signature of Employee Date

_ Employee refused to sign appraisal

Rating Official _____ Date: _____

4

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

A Special Investigative Panel

President's Foreign Intelligence Advisory Board

JUNE 1999

TABLE OF CONTENTS

ABSTRACT, FOREWORD

FINDINGS

ROOT CAUSES

- An International Enterprise
- Big, Byzantine, and Bewildering Bureaucracy
- Lack of Accountability
- Culture and Attitudes
- Changing Times, Changing Missions

RECURRING VULNERABILITIES

Management and Planning
Physical Security
Screening and Monitoring Personnel
Protection of Classified and Sensitive Information
Tracking Nuclear Materials
Foreign Visitors' Program

ASSESSMENTS

Responsibility
Record of the Clinton Team
The 1995 "Walk-In" Document
W-88 Investigation
Damage Assessment
PDD-61: Birth and Intent
Timeliness of PDD-61
Secretary Richardson's Initiatives
Prospects for Reforms
Trouble Ahead
Back to the Future

REORGANIZATION

Leadership
Restructuring

RECOMMENDATIONS

APPENDIX

Chronology of Events
Chronology of Reports on DOE
Damage Assessment of China's Acquisition of U.S. Nuclear Information
Presidential Decision Directive 61
Bibliography
Map of DOE Installations

PANEL MEMBERS

The Honorable Warren B. Rudman, Chairman of the President's Foreign Intelligence Advisory Board. Senator Rudman is a partner in the law firm of Paul, Weiss, Rifkind, Wharton, and Garrison. From 1980 to 1992, he served in the U.S. Senate, where he was a member of the Select Committee on Intelligence. Previously, he was Attorney General of New Hampshire.

Ms. Ann Z. Caracristi, board member. Ms. Caracristi, of Washington, DC, is a former Deputy Director of the National Security Agency, where she served in a variety of senior management positions over a 40–year career. She is currently a member of the DCI/Secretary of Defense Joint Security Commission and recently chaired a DCI Task Force on intelligence training. She was a member of the Aspin/Brown Commission on the Roles and Capabilities of the Intelligence Community.

Dr. Sidney D. Drell, board member. Dr. Drell, of Stanford, California is an Emeritus Professor of Theoretical Physics and a Senior Fellow at the Hoover Institution. He has served as a scientific consultant and advisor to several congressional committees, The White House, DOE, DOD, and the CIA. He is a member of the National Academy of Sciences and a past President of the American Physical Society.

Mr. Stephen Friedman, board member. Mr. Friedman is Chairman of the Board of Trustees of Columbia University and a former Chairman of Goldman, Sachs, & Co. He was a member of the Aspin/Brown Commission on the Roles and Capabilities of the Intelligence Community and the Jeremiah Panel on the National Reconnaissance Office.

PFIAB STAFF

Randy W. Deitering, *Executive Director*

Mark F. Moynihan, *Assistant Director*

Roosevelt A. Roy, *Administrative Officer*

Frank W. Fountain, *Assistant Director and Counsel*

Brendan G. Melley, *Assistant Director*

Jane E. Baker, *Research/Administrative Officer*

PFIAB ADJUNCT STAFF

Roy B., *Defense Intelligence Agency*

Karen DeSpiegelaere, *Federal Bureau of Investigation*

Jerry L., *Central Intelligence Agency*

Christine V., *Central Intelligence Agency*

David W. Swindle, *Department of Defense, Naval Criminal Investigative Service*

Joseph S. O'Keefe, *Department of Defense, Office of the Secretary of Defense*

FAS | Secrecy | Library ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

A Special Investigative Panel

President's Foreign Intelligence Advisory Board

JUNE 1999

ABSTRACT

On March 18, 1999, President William J. Clinton requested that the President's Foreign Intelligence Advisory Board (PFIAB) undertake an inquiry and issue a report on "the security threat at the Department of Energy's weapons labs and the adequacy of the measures that have been taken to address it."

Specifically, the President asked the PFIAB to "address the nature of the present counterintelligence security threat, the way in which it has evolved over the last two decades and the steps we have taken to counter it, as well as to recommend any additional steps that may be needed." He also asked the PFIAB "to deliver its completed report to the Congress, and to the fullest extent possible consistent with our national security, release an unclassified version to the public."

In response, the Honorable Warren B. Rudman, Chairman of PFIAB, appointed board members Ms. Ann Z. Caracristi, Dr. Sidney Drell, and Mr. Stephen Friedman to form the Special Investigative Panel and

obtained detailees from several federal agencies (CIA, DOD, FBI) to augment the work of the PFIAB staff. Over the past three months, the panel and staff interviewed more than 100 witnesses, reviewed more than 700 documents encompassing thousands of pages, and conducted onsite research and interviews at five of the Department of Energy's national laboratories and plants: Livermore, Los Alamos, Oak Ridge, Pantex, and Sandia.

The panel has produced a report and an appendix of supporting documents, both of which are unclassified to the fullest extent possible. A large volume of classified material, which was also reviewed and distilled for this report, has been relegated to a second appendix that is available only to authorized recipients. This report examines:

- The 20–year history of security and counterintelligence issues at the DOE national laboratories, with an emphasis on the five labs that focus on weapons–related research;
- The inherent tension between security concerns and scientific freedom at the labs and its effect on the institutional culture and efficacy of the Department;
- The growth and evolution of the foreign intelligence threat to the national labs, particularly in connection with the Foreign Visitor's Program of the labs;
- The implementation and effectiveness of Presidential Decision Directive No. 61, the reforms instituted by Secretary of Energy Bill Richardson, and other related initiatives; and,
- Additional measures that should be taken to improve security and counterintelligence at the labs.

FOREWORD FROM THE SPECIAL INVESTIGATIVE PANEL

For the past two decades, the Department of Energy has embodied science at its best and security of secrets at its worst.

Within DOE are a number of the crown jewels of the world's government–sponsored scientific research and development organizations. With its record as the incubator for the work of many talented scientists and engineers—including many Nobel prize winners—DOE has provided the nation with far–reaching advantages. Its discoveries not only helped the United States to prevail in the Cold War, they undoubtedly will continue to provide both technological benefits and inspiration for the progress of generations to come. The vitality of its national laboratories is derived to a great extent from their ability to attract talent from the widest possible pool, and they should continue to capitalize on the expertise of immigrant scientists and engineers. However, we believe that the dysfunctional structure at the heart of the Department has too often resulted in the mismanagement of security in weapons–related activities and a lack of emphasis on counterintelligence.

DOE was created in 1977 and heralded as the centerpiece of the federal solution to the energy crisis that had stunned the American economy. A vital part of this new initiative was the Energy Research and Development Administration (ERDA), the legacy agency of the Atomic Energy Commission (AEC) and inheritor of the national programs to develop safe and reliable nuclear weapons. The concept, at least, was straightforward: take the diverse and dispersed energy research centers of the nation, bring them under an umbrella organization with other energy–related enterprises, and spark their scientific progress through closer contacts and centralized management.

At the birth of DOE, the brilliant scientific breakthroughs of the nuclear weapons laboratories came with a troubling record of security administration. Twenty years later, virtually every one of its original problems persists.

However, the brilliant scientific breakthroughs at the nuclear weapons laboratories came with a very troubling record of security administration. For example, classified documents detailing the designs of the most advanced nuclear weapons were found on library shelves accessible to the public at the Los Alamos laboratory. Employees and researchers were receiving little, if any, training or instruction regarding espionage threats. Multiple chains of command and standards of performance negated accountability, resulting in pervasive inefficiency, confusion, and mistrust. Competition among laboratories for contracts, and among researchers for talent, resources, and support distracted management from security issues. Fiscal management was bedeviled by sloppy accounting. Inexact tracking of the quantities and flows of nuclear materials was a persistent worry. Geographic decentralization fractured policy implementation and changes in leadership regularly depleted the small reservoirs of institutional memory. Permeating all of these issues was a prevailing cultural attitude among some in the DOE scientific community that regarded the protection of nuclear know–how with either fatalism or naiveté.

Twenty years later, every one of these problems still existed. Most still exist today.

In response to these problems, the Department has been the subject of a nearly unbroken history of dire warnings and attempted but aborted reforms. A cursory review of the open-source literature on the DOE record of management presents an abysmal picture. Second only to its world–class intellectual feats has been its ability to fend off systemic change. Over the last dozen years, DOE has averaged some kind of major departmental shake–up every two to three years. No President, Energy Secretary, or Congress has been able to stem the recurrence of fundamental problems. All have been thwarted time after time by the intransigence of this institution. The Special Investigative Panel found a large organization saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial. For instance, even after President Clinton issued Presidential Decision Directive 61 *ordering* that the Department make fundamental changes in security procedures, compliance by Department bureaucrats was grudging and belated.

The panel found a department saturated with cynicism, an arrogant disregard for authority, and a staggering pattern of denial.

Time after time over the past few decades, officials at DOE headquarters and the weapons labs themselves have been presented with overwhelming evidence that their lackadaisical oversight could lead to an increase in the nuclear threat against the United States. Throughout its history, the Department has been the subject of scores of critical reports from the General Accounting Office (GAO), the intelligence community, independent commissions, private management consultants, its Inspector General, and its own security experts. It has repeatedly attempted reforms. Yet the Department's ingrained behavior and values have caused it to continue to falter and fail.

PROSPECTS FOR REFORMS

We believe that Secretary of Energy Richardson, in attempting to deal with many critical security matters facing the Department, is on the right track in some, though not all, of his changes. We concur with and encourage many of his recent initiatives, and we are heartened by his aggressive approach and command

of the issues. But we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

After a review of more than 700 reports and studies, thousands of pages of classified and unclassified source documents, interviews with scores of senior federal officials, and visits to several of the DOE laboratories at the heart of this inquiry, the Special Investigative Panel has concluded the Department of Energy is incapable of reforming itself—bureaucratically and culturally—in a lasting way, even under an activist Secretary.

The panel has found that DOE and the weapons laboratories have a deeply rooted culture of low regard for and, at times, hostility to security issues, which has continually frustrated the efforts of its internal and external critics, notably the GAO and the House Energy and Commerce Committee. Therefore, a reshuffling of offices and lines of accountability may be a necessary step toward meaningful reform, but it almost certainly will not be sufficient.

Even if every aspect of the ongoing structural reforms is fully implemented, the most powerful guarantor of security at the nation's weapons laboratories will not be laws, regulations, or management charts. It will be the attitudes and behavior of the men and women who are responsible for the operation of the labs each day. These will not change overnight, and they are likely to change only in a different cultural environment—one that values security as a vital and integral part of day–to–day activities and believes it can coexist with great science.

We are convinced that when Secretary Richardson vacates the office his successor is not likely to have a comparable appreciation of the gravity of the Department's past problems, nor a comparable interest in resolving them. The next Secretary of Energy will not have spent months at the tip of the sword created by the recent public outcry over DOE mismanagement of national secrets. Indeed, the core of the Department's bureaucracy is quite capable of undoing Secretary Richardson's reforms, and may well be inclined to do so if given the opportunity.

Ultimately, the nature of the institution and the structure of the incentives under a culture of scientific research require great attention if they are to be made compatible with the levels of security and the degree of command–and–control warranted where the research and stewardship of nuclear weaponry is concerned. Yet it must be done.

THE PFIAB INQUIRY

The PFIAB panel is fully aware of the many recent allegations of management failures surrounding the Department of Energy and questions about the subsequent roles of entities such as the Department of Justice, the Federal Bureau of Investigation, and the Central Intelligence Agency. Much of the research we conducted has relevance to these allegations. However, the depth and the complexity of the issues call for examinations by institutions with greater resources and a wider charter: namely, Congress and standing executive agencies of the federal government.

In the 90 days of our inquiry, the PFIAB panel conducted numerous interviews with senior federal officials who agreed to speak candidly—with the understanding that they would not be identified by name—about DOE's problems and recent events. On balance, the panel finds that some very damaging security compromises may have occurred, as alleged by some in recent weeks. But we believe that in matters of intelligence and counterintelligence, one cannot brush off the reality that conclusions are often intrinsically based on probabilities, rather than certainties.

Leaders, of course, are often obliged to act, and should act, based on the probability of impending danger,

not only its certainty. And those entrusted with the public weal are indisputably served better by having more information about risks than less. So the panel would like to note the contributions of those who have helped to raise the public's awareness of the risks to national security posed by problems at DOE. Although we do not concur with all of their conclusions, we believe that both intelligence officials at the Department of Energy and the members of the Cox Committee made substantial and constructive contributions to understanding and resolving security problems at DOE. As we note later in this report, we concur on balance with the damage assessment of espionage losses conducted by the Director of Central Intelligence. We also concur with the findings of the independent review of that assessment by Admiral David Jeremiah and his panel.

Our mandate from President Clinton was restricted to an analysis of the structural and management problems in the Department's security and counterintelligence operations. We abided by that. We also recognize the unique nature of the assignment given to us by the President. Never before in its history of more than 35 years has the PFIAB prepared a report for release to the general public. As a result, we have taken pains to ensure that the language of this report is "plain English," not bureaucratese, and that the findings of the report are stated directly and candidly, not with the indirection and euphemisms often employed by policy insiders.

SOLUTIONS

Our panel has concluded that the Department of Energy, when faced with a profound public responsibility, has failed. Therefore, this report suggests two alternative organizational solutions, both of which we believe would substantially insulate the weapons laboratories from many of DOE's historical problems and promote the building of a responsible culture over time. We also offer recommendations for improving various aspects of security and counterintelligence at DOE, such as personnel assurance, cyber–security, program management, and interdepartmental cooperation under the Foreign Intelligence Surveillance Act of 1978.

The weapons research and stockpile management functions should be placed wholly within a new semi–autonomous agency within DOE that has a clear mission, streamlined bureaucracy, and drastically simplified lines of authority and accountability. Useful lessons along these lines can be taken from the National Security Agency (NSA) or Defense Advanced Research Projects Agency (DARPA) within the Department of Defense or the National Oceanographic and Atmospheric Administration (NOAA) within the Department of Commerce. The other alternative is a wholly independent agency, such as the National Aeronautics and Space Administration (NASA). There was substantial debate among the members of the panel about these two alternatives. Both have strengths and weaknesses. In the final analysis, the decision rests in the hands of the President and the Congress, and we trust that they will give serious deliberation to the merits and shortcomings of the alternatives before enacting major reforms. We all agree, nonetheless, that the labs should never be subordinated to the Department of Defense.

With either proposal it will be important for the weapons labs to maintain effective scientific contact on nonclassified scientific research with the other DOE labs and the wider scientific community. To do otherwise would work to the detriment of the nation's scientific progress and security over the long run. This argument draws on history: nations that honor and advance freedom of inquiry have fared better than those who have sought to arbitrarily suppress and control the community of science.

The nuclear weapons and research functions of DOE need more autonomy, a clearer mission, a streamlined bureaucracy, and increased accountability.

However, we would submit that we do not face an either/or proposition. The past 20 years have provided a controlled experiment of a sort, the results of which point to institutional models that hold promise. Organizations such as NASA and DARPA have advanced scientific and technological progress while maintaining a respectable record of security. Meanwhile, the Department of Energy, with its decentralized structure, confusing matrix of cross–cutting and overlapping management, and shoddy record of accountability has advanced scientific and technological progress, but at the cost of an abominable record of security with deeply troubling threats to American national security.

Thomas Paine once said that "government, even in its best state, is but a necessary evil; in its worst state, an intolerable one." This report finds that DOE's performance, throughout its history, should have been regarded as intolerable.

We believe the results and implications of this experiment are clear. It is time for the nation's leaders to act decisively in the defense of America's national security.

Warren Rudman
Chairman of the President's Foreign
Intelligence Advisory Board

Ms. Ann Caracristi
Board Member

Dr. Sidney Drell
Board Member

Mr. Stephen Friedman
Board Member

On To Next Section

Back To Top Page of Report

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

FINDINGS

On March 18, 1999, President Clinton tasked the Foreign Intelligence Advisory Board to review the history of the security and counterintelligence threats to the nation's weapons labs and the effectiveness of the responses by the U.S. government. He also asked the Board to propose further improvements.

This report, based on reviews of hundreds of source documents and studies, analysis of intelligence reports, and scores of interviews with senior level officials from several administrations, was prepared over the past 90 days in fulfillment of the President's request.

BOTTOM LINE

Our bottom line: DOE represents the best of America's scientific talent and achievement, but it has also been responsible for the worst security record on secrecy that the members of this panel have ever encountered.

The national labs of the Department of Energy are among the crown jewels of the world's government–sponsored scientific research and development organizations. With its record as the incubator for the work of many talented scientists and engineers—including many Nobel prize winners—it has provided the nation with far–reaching advantages. Its discoveries not only helped the United States to prevail in the Cold War, they will undoubtedly provide both technological benefits and inspiration for the progress of generations to come. Its vibrancy is derived to a great extent from its ability to attract talent from the widest possible pool, and it should continue to capitalize on the expertise of immigrant scientists and engineers. However, the Department has devoted far too little time, attention, and resources to the prosaic but grave responsibilities of security and counterintelligence in managing its weapons and other national security programs.

FINDINGS

The preponderance of evidence accumulated by the Special Investigative Panel, spanning the past 25 years, has compelled the members to reach many definite conclusions—some very disturbing—about the security and well–being of the nation's weapons laboratories.

As the repository of America's most advanced know-how in nuclear and related armaments and the home of some of America's finest scientific minds, these labs have been and will continue to be a major target of foreign intelligence services, friendly as well as hostile. Two landmark events, the end of the

Cold War and the overwhelming victory of the United States and its allies in the Persian Gulf War, markedly altered the security equations and outlooks of nations throughout the world. Friends and foes of the United States intensified their efforts to close the technological gap between their forces and those of America, and some redoubled their efforts in the race for weapons of mass destruction. Under the restraints imposed by the Comprehensive Test Ban Treaty, powerful computers have replaced detonations as the best available means of testing the viability and performance capabilities of new nuclear weapons. So research done by U.S. weapons laboratories with high performance computers stands particularly high on the espionage hit list of other nations, many of which have used increasingly more sophisticated and diverse means to obtain the secrets necessary to join the nuclear club.

Snapshot: DOE Weapons Operations

Percentage of Budget: Roughly $6 billion, a third of the Department's $18 billion FY99 budget.

Allocation of Weapons-Related Budget:

Defense Programs	$4.4 billion
Nonproliferation/Nat. Sec.	0.7
Fissile Material Disposal	0.2
Naval Reactors	0.7

Number of Contract Employees: 34,190

Number of Contract Employees Per Lab

Los Alamos	6,900
Sandia	7,500
L. Livermore	6,400
Pantex	2,860
Oak Ridge (Y-12)	5,500
Kansas City	3,150
Nevada Test Site	1,880

SOURCE: DEPT. OF ENERGY FIELD FACTBOOK, MAY 1998

More than 25 years worth of reports, studies and formal inquiries—by executive branch agencies, Congress, independent panels, and even DOE itself—have identified a multitude of chronic security and counterintelligence problems at all of the weapons labs (See Appendix). These reviews produced scores of stern, almost pleading, entreaties for change. Critical security flaws—in management and planning, personnel assurance, some physical security areas, control of nuclear materials, protection of documents and computerized information, and counterintelligence—have been cited for immediate attention and resolution ... over and over and over ... ad nauseam.

The open–source information alone on the weapons laboratories overwhelmingly supports a troubling conclusion: their security and counterintelligence operations have been seriously hobbled and relegated to low-priority status for decades. The candid, closed–door testimony of current and former federal officials as well as the content of voluminous classified materials received by this panel in recent weeks reinforce this conclusion. When it comes to a genuine understanding of and appreciation for the value of security and counterintelligence programs, especially in the context of America's nuclear arsenal and secrets, the DOE and its weapons labs have been Pollyannaish. The predominant attitude toward security and counterintelligence among many DOE and lab managers has ranged from half–hearted, grudging accommodation to smug disregard. Thus the panel is convinced that the potential for major leaks and thefts of sensitive information and material has been substantial. Moreover, such security lapses would have occurred in bureaucratic environments that would have allowed them to go undetected with relative ease.

Organizational disarray, managerial neglect, and a culture of arrogance—both at DOE headquarters and the labs themselves—conspired to create an espionage scandal waiting to happen. The physical security efforts of the weapons labs (often called the "guns, guards, and gates") have had some isolated shortcomings, but on balance they have developed some of the most advanced security technology in the world. However, perpetually weak systems of personnel assurance, information security, and counterintelligence have invited attack by foreign intelligence services. Among the defects this panel found:

- Inefficient personnel clearance programs, wherein haphazard background investigations could take years to complete and the backlogs numbered in the tens of thousands.
- Loosely controlled and casually monitored programs for thousands of unauthorized foreign scientists and assignees—despite more than a decade of critical reports from the General Accounting Office, the DOE Inspector General, and the intelligence community.
- This practice occasionally created bizarre circumstances in which regular lab employees with security clearances were supervised by foreign nationals on temporary assignment.
- Feckless systems for control of classified documents, which periodically resulted in thousands of documents being declared lost.
- Counterintelligence programs with part–time CI officers, who often operated with little experience, minimal budgets, and employed little more than crude "awareness" briefings of foreign threats and perfunctory and sporadic debriefings of scientists travelling to foreign countries.
- A lab security management reporting system that led everywhere but to responsible authority.
- Computer security methods that were naive at best and dangerously irresponsible at worst.

Why were these problems so blatantly and repeatedly ignored? DOE has had a dysfunctional management structure and culture that only occasionally gave proper credence to the need for rigorous security and counterintelligence programs at the weapons labs. For starters, there has been a persisting lack of real leadership and effective management at DOE.

The nature of the intelligence–gathering methods used by the People's Republic of China poses a special challenge to the U.S. in general and the weapons labs in particular. More sophisticated than some of the blatant methods employed by the former Soviet bloc espionage services, PRC intelligence operatives know their strong suits and play them extremely well. Increasingly more nimble, discreet and transparent in their spying methods, the Chinese services have become very proficient in the art of seemingly innocuous elicitations of information. This modus operandi has proved very effective against unwitting and ill–prepared DOE personnel.

Despite widely publicized assertions of wholesale losses of nuclear weapons technology from specific laboratories to particular nations, the factual record in the majority of cases regarding the DOE weapons laboratories supports plausible inferences—but not irrefutable proof—about the source and scope of espionage and the channels through which recipient nations received information. The panel was not charged, nor was it empowered, to conduct a technical assessment regarding the extent to which alleged losses at the national weapons laboratories may have directly advanced the weapons development programs of other nations. However, the panel did find these allegations to be germane to issues regarding the structure and effectiveness of DOE security programs, particularly the counterintelligence functions.

The classified and unclassified evidence available to the panel, while pointing out systemic security vulnerabilities, falls short of being conclusive. The actual damage done to U.S. security interests is, at the least, currently unknown; at worst, it may be unknowable. Numerous variables are inescapable. Analysis of indigenous technology development in foreign research laboratories is fraught with uncertainty. Moreover, a nation that is a recipient of classified information is not always the sponsor of the espionage by which it was obtained. However, the panel does concur, on balance, with the findings of the recent DCI–sponsored damage assessment. We also concur with the findings of the subsequent independent review, led by retired Admiral David Jeremiah, of that damage assessment.

The Department of Energy is a dysfunctional bureaucracy that has proven it is incapable of reforming itself. Accountability at DOE has been spread so thinly and erratically that it is now almost impossible to find. The long traditional and effective method of entrenched DOE and lab bureaucrats is to defeat security reform initiatives by waiting them out. They have been helped in this regard by the frequent changes in leadership at the highest levels of DOE—nine Secretaries of Energy in 22 years. Eventually, the reform–minded management transitions out, either due to a change in administrations or as a result of the traditional "revolving door" management practices at DOE. Then the bureaucracy reverts to old priorities and predilections. Such was the case in December 1990 with the reform recommendations carefully crafted by a special task force commissioned by then–Energy Secretary Watkins. The report skewered DOE for unacceptable "direction, coordination, conduct, and oversight" of safeguards and security. Two years later, the new administration rolled in, redefined priorities, and the initiatives all but evaporated. Deputy Secretary Charles Curtis in late 1996 investigated clear indications of serious security and CI problems and drew up a list of initiatives in response. Those initiatives also were dropped after he left office.

Reorganization is clearly warranted to resolve the many specific problems with security and counterintelligence in the weapons laboratories, but also to address the lack of accountability that has become endemic throughout the entire Department. Layer upon layer of bureaucracy, accumulated over the years, has diffused responsibility to the point where scores claim it, no one has enough to make a difference, and all fight for more. Convoluted, confusing, and often contradictory reporting channels make the relationship between DOE headquarters and the labs, in particular, tense, internecine, and chaotic. In between the headquarters and the laboratories are field offices, which the panel found to be a locus of much confusion. In background briefings of the panel, senior DOE officials often described them as redundant operations that function as a shadow headquarters, often using their political clout and large payrolls to push their own agendas and budget priorities in Congress. Even with the latest DOE restructuring, the weapons labs are reporting to far too many DOE masters.

The criteria for the selection of Energy Secretaries have been inconsistent in the past. Regardless of the outcome of ongoing or contemplated reforms, the minimum qualifications for an Energy Secretary should include experience in not only energy and scientific issues, but national security and intelligence issues as well. The list of former Secretaries, Deputy Secretaries, and Under Secretaries meeting all of these criteria is very short. Despite having a large proportion of its budget (roughly 30 percent) devoted to functions related to nuclear weapons, the Department of Energy has often been led by men and women with little expertise and background in national security. The result has been predictable: security issues have been a low priority, and leaders unfamiliar with these issues have delegated decisionmaking to lesser–ranking officials who lacked the incentives and authority to address problems with dispatch and forcefulness. For a Department in desperate need of strong leadership on security issues, this has been a disastrous trend. The bar for future nominees at the upper levels of the Department needs to be raised significantly.

DOE cannot be fixed with a single legislative act: management must follow mandate. The research functions of the labs are vital to the nation's long term interest, and instituting effective gates between weapons and nonweapons research functions will require both disinterested scientific expertise,

judicious decisionmaking, and considerable political finesse. Thus both Congress and the executive branch—whether along the lines suggested by the Special Investigative Panel or others—should be prepared to monitor the progress of the Department's reforms for years to come. This panel has no illusions about the future of security and counterintelligence at DOE. There is little reason to believe future DOE Secretaries will necessarily share the resolve of Secretary Richardson, or even his interest. When the next Secretary of Energy is sworn in, perhaps in the spring of 2001, the DOE and lab bureaucracies will still have advantages that could give them the upper hand: time and proven skills at artful dodging and passive intransigence.

The Foreign Visitors' and Assignments Program has been and should continue to be a valuable contribution to the scientific and technological progress of the nation. Foreign nationals working under the auspices of U.S. weapons labs have achieved remarkable scientific advances and contributed immensely to a wide array of America's national security interests, including nonproliferation. Some have made contributions so unique that they are all but irreplaceable. The value of these contacts to the nation should not be lost amid the attempt to address deep, well–founded concerns about security lapses. That said, DOE clearly requires measures to ensure that legitimate use of the research laboratories for scientific collaboration is not an open door to foreign espionage agents. Losing national security secrets should never be accepted as an inevitable cost of obtaining scientific knowledge.

In commenting on security issues at DOE, we believe that both Congressional and Executive Branch leaders have resorted to simplification and hyperbole in the past few months. The panel found neither the dramatic damage assessments nor the categorical reassurances of the Department's advocates to be wholly substantiated. We concur with and encourage many of Secretary Richardson's recent initiatives to address the security problems at the Department, and we are heartened by his aggressive approach and command of the issues. He has recognized the organizational dysfunction and cultural vagaries at DOE and taken strong, positive steps to try to reverse the legacy of more than 20 years of security mismanagement. However, the Board is extremely skeptical that any reform effort, no matter how well–intentioned, well–designed, and effectively applied, will gain more than a toehold at DOE, given its labyrinthine management structure, fractious and arrogant culture, and the fast–approaching reality of another transition in DOE leadership. Thus we believe that he has overstated the case when he asserts, as he did several weeks ago, that "Americans can be reassured: our nation's nuclear secrets are, today, safe and secure."

Similarly, the evidence indicating widespread security vulnerabilities at the weapons laboratories has been ignored for far too long, and the work of the Cox Committee and intelligence officials at the Department has been invaluable in gaining the attention of the American public and in helping focus the political will necessary to resolve these problems. Nonetheless, there have been many attempts to take the valuable coin of damaging new information and decrease its value by manufacturing its counterfeit, innuendo; possible damage has been minted as probable disaster; workaday delay and bureaucratic confusion have been cast as diabolical conspiracies. Enough is enough.

Fundamental change in DOE's institutional culture—including the ingrained attitudes toward security among personnel of the weapons laboratories—will be just as important as organizational redesign. Never have the members of the Special Investigative Panel witnessed a bureaucratic culture so thoroughly saturated with cynicism and disregard for authority. Never before has this panel found such a cavalier attitude toward one of the most serious responsibilities in the federal government—control of the design information relating to nuclear weapons. Particularly egregious have been the failures to enforce cyber–security measures to protect and control important nuclear weapons design information. Never before has the panel found an agency with the bureaucratic insolence to dispute, delay, and resist implementation of a Presidential directive on security, as DOE's bureaucracy tried to do to the Presidential Decision Directive No. 61 in February 1998.

The best nuclear weapons expertise in the U.S. government resides at the national weapons labs, and this asset should be better used by the intelligence community. For years, the PFIAB has been keen on honing the intelligence community's analytic effectiveness on a wide array of nonproliferation areas, including nuclear weapons. We believe that the DOE Office of Intelligence, particularly its analytic component, has historically been an impediment to this goal because of its ineffective attempts to manage the labs' analysis. The office's mission and size (about 70 people) is totally out of step with the Department's intelligence needs. A streamlined intelligence liaison body, much like Department of Treasury's Office of Intelligence Support—which numbers about 20 people, including a 24–hour watch team—would be far more appropriate. It should concentrate on making the intelligence community, which has the preponderance of overall analytic experience, more effective in fulfilling the DOE's analysis and collection requirements.

On to Next Section

Back to Report Top Page

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the
U.S. Department of Energy

ROOT CAUSES

The sources of DOE's difficulties in both overseeing scientific research and maintaining security are numerous and deep. The Special Investigative Panel primarily focused its inquiry on the areas within DOE where the tension between science and security is most critical: the nuclear weapons laboratories.[1] To a lesser extent, the panel examined security issues in other areas of DOE and broad organizational issues that have had a bearing on the functioning of the laboratories.

Inherent in the work of the weapons laboratories, of course, is the basic tension between scientific inquiry, which thrives on freewheeling searches for and wide dissemination of information, and governmental secrecy, which requires just the opposite. But the historical context in which the labs were created and thrived has also figured into their subsequent problems with security.

AN INTERNATIONAL ENTERPRISE

U.S. research laboratories have always had a tradition of drawing on immigrant talent. Perhaps the first foreign–born contributor to our nation's nuclear program was Albert Einstein. In his letter to President Roosevelt on August 2, 1939, Einstein advised the President of the possibility of the atomic bomb and the urgent need for government action. By 1943, the ranks of the Manhattan project at Los Alamos, New Mexico were filled with scientists and engineers from Italy (Fermi), Germany (Bethe), Poland (Ulam), Hungary (Wigner, Szilard, Von Neumann, and Teller), Russia (Kistiakovsy) and Austria (Rabi). Indeed, it is possible that the atomic bomb would never have been completed but for immigrant talent, and the diversity of talent applied to the project was hailed at the time as a model of international cooperation. Eleanor Roosevelt, in a 1945 radio address, declared that the development of the atomic bomb by "many minds belonging to different races and different religions sets the pattern for the way in which in the future we may be able to work out our difficulties."[2]

The role of and reliance on immigrant talent in the United States—particularly at the graduate school and doctoral levels where much of the nation's research is performed—has increased over the years. From 1975 to 1992, the aging of America's baby boomers resulted in a decline in the overall size of the college–age population and, unlike other industrialized nations, the U.S. saw a decline in the number of American students receiving science and engineering degrees.[3]

From the 1950s until 1995, the number of non–U.S. citizens who earned doctorates in scientific and engineering fields from American universities steadily climbed, reaching 27 percent by 1985 and 40

percent by 1995. Two–thirds of those receiving those doctorates in 1995 held temporary residency visas, and Chinese doctoral recipients outnumbered recipients from all other regions combined.[4]

But the willingness to draw on foreign talent also has meant a greater risk of falling prey to those with foreign allegiances. One of the earliest and most infamous espionage scandals at the nation's nuclear laboratories was centered on the physicist Klaus Fuchs, a German native and naturalized British citizen who spied on researchers at Los Alamos for the Soviet Union. More recent instances of actual and alleged foreign espionage at the nuclear weapons laboratories are detailed in the Classified Appendix to this report.

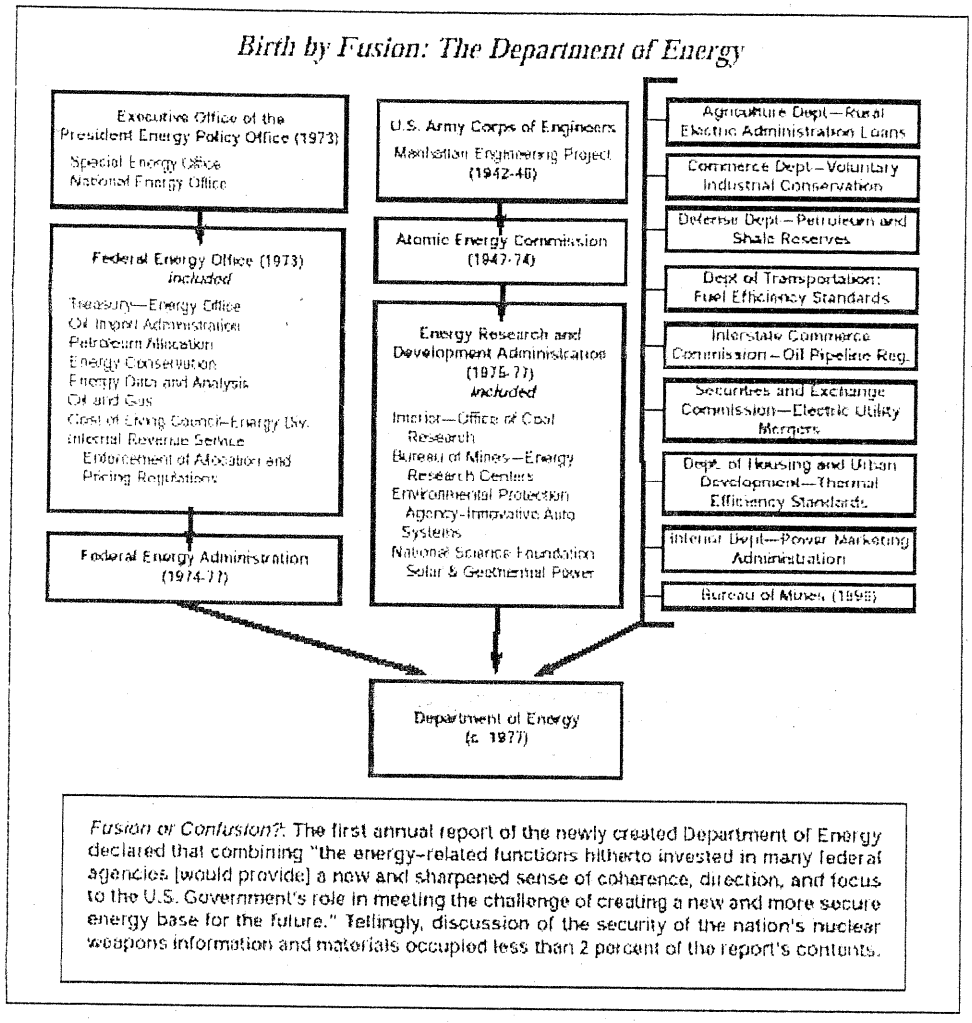
As growth of the U.S. talent pool in science and engineering stagnated, and the amount of available talent abroad grew rapidly, the U.S. has had to rely on more foreign–born talent in national scientific research and development programs in order to maintain the best research facilities in the world. At the same time, since the end of the Cold War, DOE has entered into more extensive cooperative programs with foreign nations in efforts to reduce the threats of proliferation and diversion of nuclear weapons material. By June 1990, DOE had entered into 157 bilateral research and development agreements for scientific exchange purposes. Among others, parties to the agreements were the Soviet Union, the People's Republic of China, Soviet bloc nations and countries that posed nuclear proliferation threats.[5] In December 1990, a report to the DOE Secretary noted "a high probability of greatly increasing numbers of foreign visits and assignments to DOE facilities in future years."[6] The widening of foreign contacts concurrent with a greater influx of foreign–born talent has raised concerns about security compromises by scientists with foreign allegiances and highlighted the need for special care in implementing formal clearance procedures for involvement in classified work.

BIG, BYZANTINE, AND BEWILDERING BUREAUCRACY

DOE is not one of the federal government's largest agencies in absolute terms, but its organizational structure is widely regarded as one of the most confusing. That is another legacy of its origins, and it has made the creation, implementation, coordination, and enforcement of consistent policies very difficult over the years.

The effort to develop the atomic bomb was managed through an unlikely collaboration of the Manhattan Engineering District of the U.S. Army Corps of Engineers (hence the name, "the Manhattan Project") and the University of California—two vastly dissimilar organizations in both culture and mission. The current form of the Department took shape in the first year of the Carter Administration through the merging of more than 40 different government agencies and organizations, an event from which it has arguably never recovered.

The newly created DOE subsumed the Federal Energy Administration, the Energy Research and Development Administration (ERDA), the Federal Power Commission, and components and programs of several other government agencies. Included were the nuclear weapons research laboratories that were part of the ERDA and, formerly, of the Atomic Energy Commission.



Many of these agencies and organizations have continued to operate under the DOE umbrella with the same organizational structure that they had prior to joining the Department.

Even before the new Department was created, concerns were raised about how high the nuclear weapons–related operations would rank among the competing priorities of such a large bureaucracy. A study of the issue completed in the last year of the Ford Administration considered three alternatives: shifting the weapons operations to the Department of Defense, creating a new freestanding agency, or keeping the program within ERDA—the options still being discussed more than 20 years later. As one critic of the DOE plan told *The Washington Post*, "Under the AEC, weapons was half the program. Under ERDA, it was one–sixth. Under DOE, it will be one–tenth. It isn't getting the attention it deserves." Although the proportions cited by that critic would prove to be inaccurate, he accurately spotted the direction of the trend.

The DOE Management Challenge

MISSION

- Lead agency for development of national energy resources and technologies.
- Responsible for the largest environmental cleanup effort in history.
- Nuclear energy and weapons research and development.
- Management of special nuclear materials stockpiles.

- Protection of highly sensitive classified and proprietary information against foreign and corporate espionage.

SIZE

- If included among the Nation's Fortune 500 firms, would rank in the top 50.
- The fourth largest landowner in the United States.
- Budget of roughly $18 billion comprises close to 3 percent of total discretionary spending at the federal level.
- Employs more than 11,000 Federal employees and more than 100,000 contract employees.
- Owns and manages more than 50 major installations spread across 2.4 million acres and 35 states.

COMPLEXITY

- A diverse workforce of military and civilian personnel; U.S. citizens and foreign nationals; career federal officials and part-time researchers; white collar bureaucrats as well as scientists and engineers specializing in narrow esoteric fields.
- Constituencies include the White House, Congress, the power industry, multinational defense and aerospace corporations, major universities, states and municipalities seeking or monitoring environmental cleanups.

During 1978, its first year of operation within the new structure, DOE already had in place more than 9,500 prime contracts and more than 1,800 financial assistance awards, which together were spread among 188 universities and more than 3,200 contractors. And the Department was growing: from 1977 to 1978, grants and contracts with university researchers posted an increase of 22 percent.[7]

LACK OF ACCOUNTABILITY

Depending on the issue at hand, a line worker in a DOE facility might be responsible to DOE headquarters in Washington, a manager in a field office in another state, a private contractor assigned to a DOE project, a research team leader from academia, or a lab director on another floor of the worker's building. For example, prior to Secretary Richardson's restructuring initiative earlier this year, a single laboratory, Sandia, was managed or accountable to nine different DOE security organizations.

Last year, after years of reports highlighting the problem of confused lines of authority, DOE was still unable to ensure the effectiveness of security measures because of its inability to hold personnel accountable. A 1998 report lamented that "short of wholesale contract termination, there did not appear to be adequate penalty/reward systems to ensure effective day–to–day security oversight at the contractor level."[8]

The problem is not only the diffuse nature of authority and accountability in the Department. It is the dynamic and often informal character of the authority that does exist. The inherently unpredictable outcomes of major experiments, the fluid missions of research teams, the mobility of individual researchers, the internal competition among laboratories, the ebb and flow of the academic community, the setting and onset of project deadlines, the cyclical nature of the federal budgeting process, and the shifting imperatives of energy and security policies dictated from the White House and Congress—all of these dynamic variables contribute to volatility in the Department's workforce and an inability to give the

weapons–related functions the priority they deserved. Newcomers, as a result, have an exceedingly hard time when they are assimilated; incumbents have a hard time in trying to administer consistent policies; and outsiders have a hard time divining departmental performance and which leaders and factions are credible. Such problems are not new to government organizations, but DOE's accountability vacuum has only exacerbated them.

Management and security problems have recurred so frequently that they have resulted in nonstop reform initiatives, external reviews, and changes in policy direction. As one observer noted in Science magazine in 1994: "Every administration sets up a panel to review the national labs. The problem is that nothing is done." The constant managerial turnover over the years has generated nearly continuous structural reorganizations and repeated security policy reversals. Over the last dozen years, DOE has averaged some kind of major departmental shake–up every two to three years. During that time, security and counterintelligence responsibilities have been "punted" from one office to the next.

CULTURE AND ATTITUDES

In the course of this inquiry, many officials interviewed by the PFIAB panel cited the scientific culture of the weapons laboratories as a factor that complicates, perhaps even undermines, the ability of the Department to consistently implement its security procedures. Although there seemed to be no universally accepted definition of the culture, nearly everyone agreed that it is distinct and pervasive.

One facet of the culture mentioned more than others is an arrogance borne of the simple fact that nuclear researchers specialize in one of the world's most advanced, challenging, and esoteric fields of knowledge. Nuclear physicists, by definition, are required to think in literally other dimensions not accessible to laymen. Thus it is not surprising that they might bridle under the restraints and regulations of administrators and bureaucrats who do not entirely comprehend the precise nature of the operation being managed.

Operating within a large, complex bureaucracy with transient leaders would only tend to accentuate a scientist's sense of intellectual superiority: if administrators have little more than a vague sense of the contours of a research project, they are likely to have little basis to know which rules and regulations constitute unreasonable burdens on the researchers' activities.

With respect to at least some security issues, the potential for conflicts over priorities is obvious. For example, how are security officials to weigh the risks of unauthorized disclosures during international exchanges if they have only a general familiarity with the cryptic jargon used by the scientists who might participate?

The prevailing culture of the weapons labs is widely perceived as contributing to security and counterintelligence problems. At the very least, restoring public confidence in the ability of the labs to protect nuclear secrets will require a thorough reappraisal of the culture within them.

CHANGING TIMES, CHANGING MISSIONS

The external pressures placed on the Department of Energy in general, and the weapons labs in particular, are also worth noting. For more than 50 years, America's nuclear researchers have operated in a maelstrom of shifting and often contradictory attitudes. In the immediate aftermath of World War II, nuclear discoveries were simultaneously hailed as a destructive scourge and a panacea for a wide array of mankind's problems. The production of nuclear arms was regarded during the 1950s and 1960s as one of the best indices of international power and the strength of the nation's military deterrent.

During the 1970s, the nation's leadership turned to nuclear researchers for solutions to the energy crisis at the same time that the general public was becoming more alarmed about the nuclear buildup and the environmental implications of nuclear facilities.

Over the past 20 years, some in Congress have repeatedly called for the dissolution of the Department of Energy, which has undoubtedly been a distraction to those trying to make long–term decisions affecting the scope and direction of the research at the labs. And in the aftermath of the Cold War, the Congress has looked to the nation's nuclear weapons labs to help in stabilizing or dismantling nuclear stockpiles in other nations.

Each time that the nation's leadership has made a major change in the Department's priorities or added another mission, it has placed additional pressure on a government agency already struggling to preserve and expand one of its most challenging historical roles: guarantor of the safety, security, and reliability of the nation's nuclear weapons.

ENDNOTES

1. The Department of Energy National Weapons Labs and Plants discussed in this report are: Lawrence Livermore National Lab, California; Los Alamos National Lab, New Mexico; Sandia National Lab, New Mexico; PANTEX Plant, Texas; Kansas City Plant, Missouri; Oak Ridge (Y-12) Plant, Tennessee.

2. Boyer, Paul. *By the Bomb's Early Light: American Thought and Culture at the Dawn of the Atomic Age*. Chapel Hill: University of North Carolina Press, 1985, p. 138.

3. National Science Foundation, "Science and Engineering Indicators," 1996.

4. National Science Foundation, "Data Brief," Vol. 1996, No. 9, August 19, 1999.

5. Classified report.

6. Classified DOE Report.

7. DOE, "Annual Report to Congress, 1978," April 1979.

8. U.S. Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

On to Next Section

Back to Report Top Page

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

RECURRING VULNERABILITIES

Over the past 20 years, six DOE security issues have received the most scrutiny and criticism from both inter-nal and external reviewers: long–term security planning and policy implementation; physical security over facili-ties and property; screening and monitoring of person-nel; protection of classified and sensitive information, particularly information that is stored electronically in the Department's computers; accounting for nuclear materials; and the foreign visitors' programs.

MANAGEMENT AND PLANNING

Management of security and counterintelligence has suffered from chronic problems since the creation of the Department of Energy in 1977. During the past decade, the mismatch between DOE's security programs and the severity of the threats faced by the Department grew more pronounced. While the number of nations possessing, developing, or seeking weapons of mass destruction continued to rise, America's reliance on foreign scientists and engineers dramatically increased, and warnings mounted about the espionage goals of other nations, DOE spending on safe-guards and security decreased by roughly one–third.[1]

The widening gap between the level of security and the severity of the threat resulted in cases where sensitive nuclear weapons information was certainly lost to espionage. In countless other instances, such information was left vulnerable to theft or duplication for long periods, and the extent to which these serious lapses may have damaged American security is incalculable. DOE's failure to respond to warnings from its own analysts, much less independent sources, underscores the depth of its managerial weakness and inability to implement legitimate policies regarding well–founded threats.

A Sample of Security Issues

MANAGEMENT AND PLANNING

- Decentralized decisionmaking undermines consistency of policies.
- Lack of control for security budget has allowed diversion of funds to other priorities.
- Department leaders with little experience in security and intelligence.
- Lack of accountability.

PHYSICAL SECURITY

- Training insufficient for some security personnel.
- Nuclear materials stored in aging buildings not designed for containment purposes.
- Recurring problems involving lost or stolen property.
- Poor management results in unnecessary training and purchasing costs.

PERSONNEL SECURITY CLEARANCES

- Extended lags in obtaining clearances, reinvestigating backgrounds, and terminating clear-ance privileges for former employees.
- Some contractors not adequately investigated or subject to drug and substance abuse policies.
- Lack of uniform procedures and accurate data.
- Inadequate pre–employment screening.
- More clearances granted than necessary.

PROTECTION OF CLASSIFIED INFORMATION

- Poor labeling and tracking of computer media containing classified information.
- Problems with lax enforcement of password policies.
- Network, email, and Internet connections make transfer of large amounts of data easier.

ACCOUNTING FOR NUCLEAR MATERIALS

- Chronic problems in devising and operating an accurate accounting system of tracking stocks and flows of nuclear materials.

FOREIGN VISITORS

- Weak systems for tracking visits and screening backgrounds of visiting scientists.
- Decentralization makes monitoring of discus-sions on sensitive topics difficult.

During the mid–1980s, the predominant concern of DOE officials was improving the physical security of the nuclear weapons laboratories and plants. Following a January 1983 report [2] that outlined vulnerabilities of the weapons labs to terrorism, the Department embarked on a five–year program of construction and purchases that would see its overall safeguards and security budget roughly double and its spending on upgrades nearly triple. Included was money for additional guards, security training, helicopters, fortified guard towers, vehicle barriers, emergency planning, and advanced alarm systems.[3]

Improving physical security in a wide array of nuclear weapons facilities whose replacement value was an estimated $100 billion [4], proved to be difficult. Reports through the late 1980s and early 1990s continued to highlight deficiencies in the management of physical security.

In the late 1980s, priorities began to shift somewhat. Listening devices were discovered in weapons–related facilities,[5] and a 1990 study advised the Department leadership of an intensifying threat from foreign espionage. Less and less able to rely on the former Soviet Union to supply technology and resources, an increasing number of states embarked on campaigns to bridge the economic and technological gap with the United States by developing indigenous capabilities in high technology areas.

The study noted that the freer movement of goods, services and information in a less hostile world "intensified the prospects and opportunities for espionage as missing pieces of critically needed information became more easily identified."[6]

An intelligence report further highlighted the changing foreign threat to the labs by noting that "new threats are emerging from nontraditional adversaries who target issues key to U.S. national security. DOE facilities and personnel remain priority targets for hostile intelligence collection."[7] Anecdotal evidence corroborates, and intelligence assessments agree, that foreign powers stepped up targeting of DOE during the early 1990s. (See Classified Appendix) While this threat may have been taken seriously at the highest levels of the DOE, it was not uniform throughout the Department.

A former FBI senior official noted in discussions with the PFIAB investigative panel that DOE lab scientists during these years appeared naive about the level of sophistication of the nontraditional threat posed by Chinese intelligence collection. The trend in openness to for-eign visitors and visits does not indicate any sense of heightened wariness. A 1997 GAO report concluded that from mid–1988 to the mid–1990s, the number of foreign visitors to key weapons labs increased from 3,800 to 5,900 annually and sensitive country visitors increased from 500 to more than 1,600. [8] Meanwhile, the DOE budget for counterintelligence was in near–constant decline.

As noted in the previous chapter, federal officials in charge of oversight of nuclear weapons laboratories have historically allowed decisionmaking on basic aspects of security to be decentralized and diffuse. With their budget spread piecemeal throughout a number of offices, security and counterintelligence officials often found themselves with a weak voice in internal bureaucratic battles and an inability to muster the authority to accomplish its goals. Indeed, an excerpt from a history of the early years of the Atomic Energy Commission, reads much like recent studies:

> Admiral Gingrich, who had just resigned as director of security [in 1949], had expressed to the Joint Committee [on Atomic Energy] a lack of confidence in the Commission's security program. Gingrich complained that decentralization of administrative functions to the field offices had left him with little more than a staff function at headquarters; even there, he said, he did not control all the activities that seemed properly to belong to the director of security.[9]

How Long Does It Take?

Each year DOE security officials compile audits to identify security lapses and vulnerabilities in the facilities and procedures of the nuclear weapons laboratories and plants. The following year, they report on whether the problems have been addressed. Given the sensitivity of what was being protected—information about how to build, miniaturize, store, and maximize the destructiveness of nuclear weapons—the numbers logged in the audits are remarkable:

11	No. of months a DOE employee was dead before Department officials realized four documents with CLASSIFIED and RESTRICTED DATA were still assigned to him.
20	No. of months before DOE officials could ensure that improperly stored classified computer media had been properly safeguarded.
24	No. of months it took to order security labels (SECRET, TOP SECRET, etc.) for mislabeled software.
31	No. of months that 2,750 out of 3,000 non-classified computer terminals were connected and being used on a classified network.
31	No. of months to write and approve a network security plan.
35	No. of months it took DOE officials to write a work order to replace a lock at a weapons lab facility containing sensitive nuclear information.
45	No. of months taken to correct a broken doorknob that was sticking in an open position and allowing access to sensitive areas.
51	No. of months to correct mistake that allowed secure telephone cryptographic materials to go improperly safeguarded.
?	No. of months before security audit team discovered that the main telephone frame room door at a weapons lab had been forced open and the lock destroyed.

SOURCE: DEPT. OF ENERGY

More than 30 years later, decentralization still posed a problem for security managers. An internal DOE report in 1990 found that the Department lacked a comprehensive approach to management of threats and dissemination of information about them.[10] A DOE annual report in 1992 found that security "has suffered from a lack of management focus and inconsistent pro-cedural execution throughout the DOE complex. The result is that personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements." [11]

The counterintelligence effort at DOE in the late 1980s and mid–1990s was in its infancy and grossly underfunded. Although the Department could have filled its gap in some areas, such as counterintelligence information, through cooperation with the broader intelligence community, PFIAB research and interviews indicate that DOE headquarters' relationship with the FBI—the United States' primary domestic CI organization—was strained at best.

DOE requested an FBI agent detailee in 1988 to assist in developing a CI program, but the agent found that DOE failed to provide management support or access to senior DOE decisionmakers. A formal relationship with the FBI was apparently not established until 1992: a Memorandum of Understanding between the FBI and DOE on respective responsibilities concerning the coordination and conduct of CI activities in the United States. However, in 1994 two FBI detailees assigned to DOE complained about their limited access and were pulled back to FBI because of a "lack of control of the CI program by DOE headquarters which resulted in futile attempts to better manage the issue of foreign visitors at the laboratories."[12]

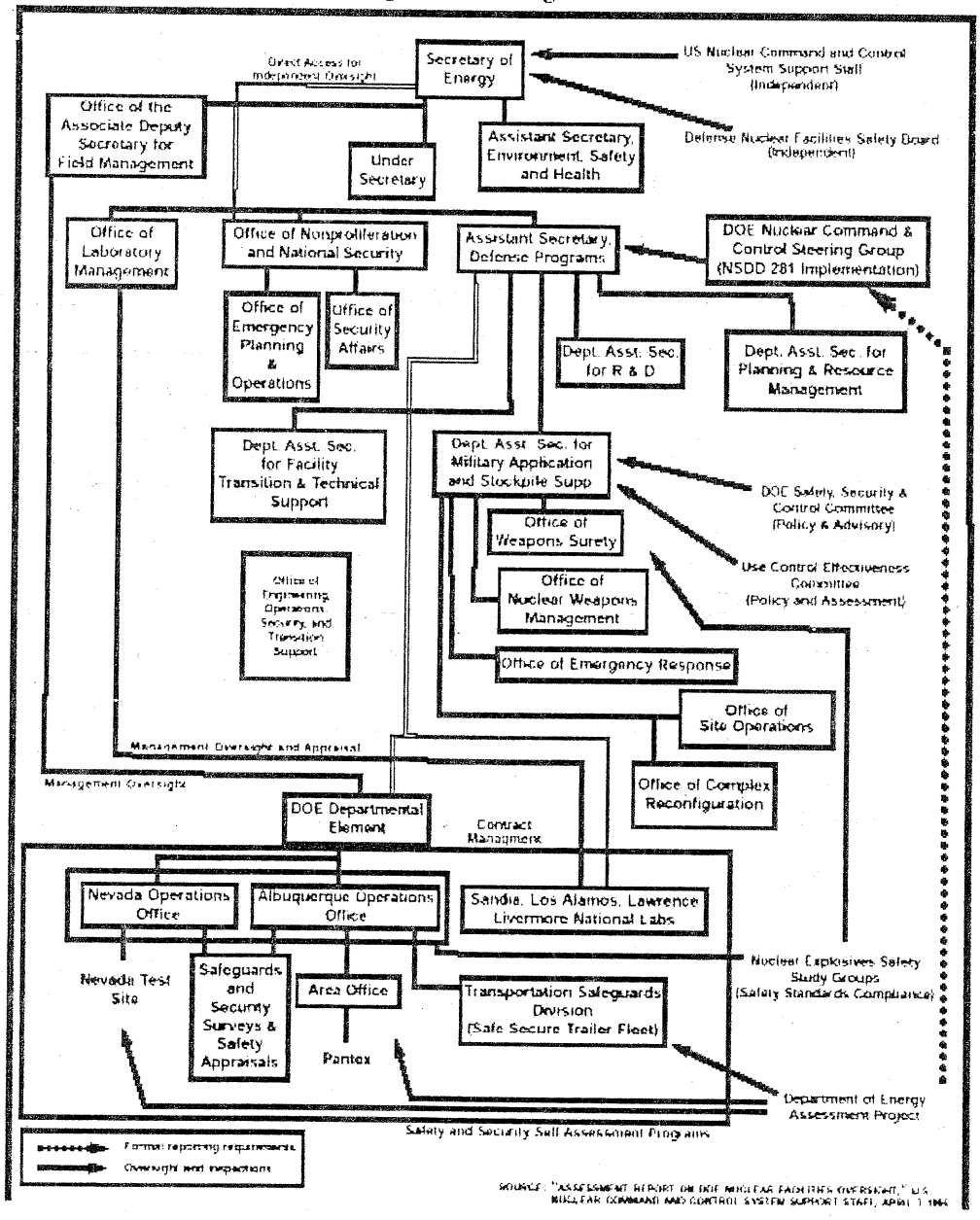
We asked a number of DOE officials to whom they report, to whom they were responsible.

Invariably, their answer was: "It depends."

The haphazard assortment of agencies and missions folded into DOE has become so confusing as to become a running joke within the institution. In the course of the panel's research and interviews, rare were the senior officials who expressed any sort of confidence in their understanding of the extent of the agency's operations, facilities, or procedures. Time and again, PFIAB panel members posed the elementary questions to senior DOE officials. To whom do you report? To whom are you accountable? The answer, invariably, was: "It depends."

DOE's relationship with the broader intelligence community was not well–defined until the mid–1990s. Coordination between DOE CI elements and the broader intelligence community, according to a 1992 intelligence report, was hampered from the 1980s through the early 1990s by DOE managers' inadequate understanding of the intelligence community.[13] The Department did not become a core member of the National Counterintelligence Policy Board (established in 1994 under PDD-24) until 1997.

DOE Nuclear Programs Management/Oversight Structure Prior to 1999 Reforms



SOURCE: "ASSESSMENT REPORT ON DOE NUCLEAR FACILITIES OVERSIGHT," U.S. NUCLEAR COMMAND AND CONTROL SYSTEM SUPPORT STAFF, APRIL 1, 1994

Over much of the past decade, rather than a heightened sensitivity to espionage threats recognized widely throughout the intelligence community, DOE lab officials have operated in an environment that allowed them to be sanguine, if not skeptical. Numerous DOE officials interviewed by the PFIAB panel stated that they believed that the threat perception was weakened further during the administration of Secretary O'Leary, who advanced the labs openness policies and downgraded security as an issue by terminating some security programs instituted by her predecessor.

Even when the CI budget was expanded in the late–1990s, the expenditures fell short of the projected increases. In Fiscal Year 1997, for example, DOE's CI budget was $3.7 million but the actual expenditures on CI were only two–thirds of that level, $2.3 million. Shortly before the 1997 GAO and FBI reports on DOE's counterintelligence posture were issued, DOE began instituting changes to beef up its counterintelligence and foreign intelligence analytic capabilities.[14]

When DOE did devote its considerable resources to security, it too often faltered in implementation. A report to the Secretary in January 1994 noted "growing confusion within the Department with respect to Headquarters' guidance for safeguards and security. At this time, there is no single office at Headquarters responsible for the safeguards and security program. Most recently, a number of program offices have substantially expanded their safeguards and security staff to office–size organizations. These multiple safeguards and security offices have resulted in duplication of guidance, unnecessary requests for information and clarification, and inefficient program execution. Unchecked, this counterproductive tendency threatens the success of the overall safeguards and security effort."[15]

A 1996 DOE Inspector General report found that security personnel at the weapons programs had purchased and stockpiled far more firepower—ranging from handguns and rifles to submachine guns and grenade launchers—than could ever be used in an actual emergency. The Oak Ridge facilities had more than three weapons per armed security officer—on and off duty. Los Alamos National Laboratory had more than four.[16]

Foreign agents could probably not shoot their way into U.S. weapons laboratories. But they could apply for an access pass to walk in and strike up a conversation.

Around the same time, GAO security audits of the research laboratories at these sites found lax procedures for issuing access passes to secure areas, inadequate prescreening of the more than 1,500 visitors from sensitive countries that visited the weapons laboratories annually, and poor tracking of the content of discussions with foreign visitors. The implication: foreign agents could probably not shoot their way past the concertina wires and bolted doors to seize secrets from U.S. weapons laboratories, but they would not need to do so. They could probably apply for an access pass, walk in the front door, and strike up a conversation.

PHYSICAL SECURITY

The physical security of the Department of Energy's weapons–related programs is roughly divided into two essential functions: tracking and control over the property and equipment within the weapons-related laboratories, and keeping unwarranted intruders out, often referred to as the realm of "guns, guards, and gates."

The general approach to security, of course, was defined by the emphasis on secrecy associated with

nuclear weapons program during World War II. Los Alamos National Laboratory was created as a "closed city"—a community with a high degree of self-sufficiency, clearly defined and protected boundaries, and a minimum of ingress from and egress to the outer world. Although the community is no longer "closed," the weapons laboratories at Los Alamos, like those at the other national laboratories, still retain formidable physical protections and barriers. In examining the history of the laboratories, the panel found only a few instances where an outsider could successfully penetrate the grounds of an operation by destruction of a physical safeguard or direct violent assault.

In visits to several of the weapons laboratories, the members of the Special Investigative Panel were impressed by the great amount of attention and investment devoted to perimeter control, weaponry, and security of building entrances and exits. Indeed, one cannot help but be struck by the forbidding and formidable garrison–type atmosphere that is prevalent at many of the facilities: barbed wire, chain–link fences, electronic sensors, and surveillance cameras. Further, the panel recognizes that the labs themselves have developed and produced some of the most sophisticated technical security devices in the world. Nonetheless, DOE reports and external reviews since at least 1984 have continued to raise concerns about aging security systems.[17]

Clearances to secure DOE areas have been granted simply for convenience, such as to reduce the length of an employee's walk from the car to the office each morning.

Management of the secure environments at the laboratories has posed more serious problems. As noted earlier, DOE may be spending too much money in some areas, buying more weapons than could conceivably be used in an emergency situation. In other cases, it may be spending too little. Budget cuts in the early and mid-1990s led to 40 to 50 percent declines in officer strength and over-reliance on local law enforcement. Resources became so low that normal protective force operations required "the use of overtime scheduling to accomplish routine site protection."[18] GAO has found an assortment of problems at Los Alamos over the past decade: security personnel failed basic tests in such tasks as firing weapons, using a baton, or handcuffing a suspect, and inaccurate and incomplete records were kept on security training.19 Other DOE facilities have had substantial problems in management of physical property.

- In 1990, Lawrence Livermore Laboratory could not account for 16 percent of its inventory of government equipment, acquired at a cost $18.6 million.[20]
- In 1993, DOE sold 57 components of nuclear reprocessing equipment and associated documents, including blueprints, to an Idaho salvage dealer. Much of what was sold was subsequently found to be potentially useful to any nation attempting to develop or advance its own reprocessing operation.[21]
- Following a GAO report in 1994, which found that the Rocky Flats facility was unable to account for large pieces of equipment such as forklifts and a semitrailer, some $21 million in inventory was written off.[22]

DOE had begun to consolidate its growing stockpile of sensitive nuclear material by 1992, but a 1997 DOE report to the Secretary found that significant quantities of the material "remain in aging buildings and structures, ranging in age from 12 to 50 years, that were never intended for use as storage facilities for extended periods."[23]

SCREENING AND MONITORING OF PERSONNEL

Insider threats to security have been a chronic problem at the nation's weapons laboratories. From the

earliest years, the importance of the labs' missions and their decentralized structure have had an uneasy coexistence with the need for thorough background investigations of researchers and personnel needing access to sensitive areas and information.

In 1947, the incoming director of security for the AEC was greeted with a backlog of more than 13,000 background investigations and a process where clearances had been dispersed to field offices that operated with few formal guidelines.[24]

Forty years later, GAO found that the backlog of personnel security investigations had increased more than nine-fold, to more than 120,000. Moreover, many clearances recorded as valid in the Department's records should have been terminated years before.[25]

Even after DOE discovered listening devices in some of its weapons laboratories, security audits found that thousands of "Q" clearances were being given to inappropriate personnel.[26]

The research of the PFIAB panel found that problems with personnel security clearances, while mitigated in some aspects, have persisted to an alarming degree. From the mid–1980s through the mid–1990s, the DOE Inspector General repeatedly warned Department officials that personnel were receiving clearances that were much higher than warranted and that outdated clearances were not being withdrawn on a timely basis. The issue became more urgent with the discovery of a clandestine surveillance device at a nuclear facility.[27]

But problems persisted. DOE Inspector General reports in 1990 and 1991 found that one of the weapons laboratories had granted "Q" clearances (which provide access to U.S. government nuclear weapons data) to more than 2,000 employees who did not need access to classified information.[28] A 1992 report to the Secretary of Energy noted that "DOE grants clearances requested by its three major defense program sponsored labs based on lab policies to clear all employees regardless of whether actual access to classified interests is required for job performance."[29]

Three years later, a review of personnel security informed the Secretary there were "individuals who held security clearances for convenience only and limited security clearances to those individuals requiring direct access to classified matter or [special nuclear materials] to perform official duties."[30]

More recent evidence is no more reassuring. A counterintelligence investigation at a nuclear facility discovered that the subject of an inquiry had been granted a "Q" clearance simply to avoid the delay caused by the normal processing of a visit.[31] That same year, an illegal telephone wiretap was discovered at the same lab. The employee who installed it confessed, but was not prosecuted by the government.[32]

PROTECTION OF CLASSIFIED AND SENSITIVE INFORMATION

Two vulnerabilities regarding classified and sensitive information at DOE have recurred repeatedly throughout the past 20 years: inappropriate release of classified information, either directly through inadvertence or indirectly through improper declassification; and the increasing mobility of classified and sensitive information through electronic media, such as computers.

As computers have progressed from the large mainframes of the 1950s and 1960s to desktop models in the 1980s and decentralized networks in the 1990s, it has become progressively easier for individuals to retrieve and transport large amounts of data from one location to another. This has presented an obvious

problem for secure environments. GAO found in 1991 that DOE inspections revealed more than 220 security weaknesses in computer systems across 16 facilities. Examples included a lack of management plans, inadequate access controls, and failures to test for compliance with security procedures.[33]

As a 1996 DOE report to the President said, "adversaries no longer have to scale a fence, defeat sensors, or bypass armed guards to steal nuclear or leading–edge 'know-how' or to shut down our critical infrastructure. They merely have to defeat the less ominous obstacles of cyber–defense."[34]

Computer systems at some DOE facilities were so easy to access that even Department analysts likened them to "automatic teller machines, [allowing] unauthorized withdrawals at our nation's expense."

DOE's cyber–defenses were, in fact, found to be "less ominous obstacles." In 1994, an internal DOE review found that despite security improvement "users of unclassified computers continue to compromise classified information due to ongoing inadequacies in user awareness training, adherence to procedures, enforcement of security policies, and DOE and [lab] line management oversight."[35] Also in 1994, a report to the Energy Secretary cited five areas of concern: "failure to properly accredit systems processing classified information, lack of controls to provide access authorities and proper password management; no configuration management; improper labeling of magnetic media; and failure to perform management reviews."[36]

Apparently, the warnings were to no avail. A year later, the annual report to the Secretary noted: "Overall, findings and surveys, much like last year, continue to reflect deficiencies in self–inspections and procedural requirements or inappropriate or inadequate site guidance ... In the area of classified matter protection and control, like last year, marking, accountability, protection, and storage deficiencies are most numerous."[37]

Some reports made extra efforts to puncture through the fog of bureaucratic language. A 1995 report to the President said: "By placing sensitive information on information systems, we increase the likelihood that inimicable interests, external and internal, will treat those systems as virtual automatic teller machines, making unauthorized withdrawals at our nation's expenses." Indeed, a report found security breaches at one of the major weapons facility in which documents with unclassified but sensitive information "were found to be stored on systems that were readily accessible to anyone with Internet access."[38] In other instances, personnel were found to be sending classified information to outsiders via an unclassified email system.[39]

Ahead of its Time

In 1986, the DOE Office of Safeguards and Quality Assessment issued an inspection report on a weapons lab that warned of shortcomings in computer security and noted that the "ability of [a] user to deliberately declassify a classified file without detection and move classified information from the secure partition to the open partition can be made available to any authorized user either on or off site."[40] The warning turned out to be on the mark. In April of this year, Energy Secretary Bill Richardson issued a statement: "While I cannot comment on the specifics, I can confirm that classified nuclear weapons computer codes at Los Alamos were transferred to an unclassified computer system. This kind of egregious security breach is absolutely unacceptable ... ."

Even though the hard evidence points to only sporadic penetrations of the labs by foreign intelligence services (*see classified appendix*), volumes of sensitive and classified information may have been lost over the years—via discarded or purloined documents; uninformed and often improperly vetted employees, and a maze of uncontrolled computer links. In one recent case discovered by PFIAB, lab officials initially refused to rectify a security vulnerability because "no probability is assigned to [a loss of sensitive information], just the allegation that it is possible."[41]

As recent as last year's annual DOE report to the President, security analysts were finding "numerous incidents of classified information being placed on unclassified systems, includ-ing several since the development of a corrective action plan in July 1998."[42]

TRACKING OF NUCLEAR MATERIALS: HOW MUCH MUF?

MUF stands for "materials unaccounted for," the official term used until the late 1970s for discrepancies in the amount of nuclear materials that can be physically located in inventory versus the amount noted in Department records. MUF (now termed with the more politic phrase "inventory differences") has been a recurring concern—and debate—in the nuclear research field since the beginning. The question at the center of the debate: if large quantities of nuclear material are impossible to measure with absolute precision, what constitutes a significant loss?

As in many questions, the answer depends on whom you ask. Officials of nuclear research facilities have argued that the scale and complexity of the processing and handling of nuclear material inevitably result in losses that are detectable but inconsequential. Outside observers have tended to be less sanguine about what constitutes a significant loss from a security standpoint. In 1976, the General Accounting Office reported that the Nuclear Regulatory Commission and the Energy Research and Development Administration (DOE's predecessor) could not account for 8,000 pounds of highly enriched uranium and plutonium. Officials of the two agencies responded that part of the accounting discrepancy could be ascribed to the statistical margin of error in their measuring equipment, the rest was probably dregs created during processing and left in machinery parts, wiping cloths, and scrap items.[43]

Critics of the agencies have pointed out that thieves could easily use the variance in statistical measures to cover their tracks, stealing an increment during each measuring period that falls just within the margin of error. They have also pointed out that if Department records are not accurate, it is impossible for anyone to estimate the stock of nuclear material at any given point, much less the difference between two levels as it proceeds from one stage of the nuclear cycle to the next. In December 1994, the Department released updated figures for the cumulative amount of MUF or inventory difference for the 50-year period beginning in 1944. The cumulative figure: 6,174 pounds. Of that amount, a cumulative total of about 10 pounds was ascribed to "accidental losses" and "approved write-offs."[44]

GAO has continued to highlight the issue since DOE has become the steward of the nation's nuclear weapons laboratories. GAO published a report in 1991 criticizing the insufficiency of the Department's measuring systems and handling procedures [45] ; in 1994, criticizing its methods of tracking exported nuclear material;[46] and in 1995, for installing a new system that was allegedly faulty.[47]

Even if accurate systems of measurement and accounting had been in place, it is not clear whether DOE officials would have been qualified to manage them effectively. A 1995 report to the President warned that "severe budget reductions, diminished technical resources, increased responsibilities, and reduced mission training ... have undermined protection of special nuclear material and restricted data."[48]

Last year, a report by an external review panel found "a lack of nuclear physical security expertise at all

levels in the oversight process; ad hoc structuring of safeguards and security functions throughout the Department, and placement of oversight functions in positions which constrain their effectiveness."[49]

The dispute over the accuracy of nuclear measurements, of course, is beyond the technical capabilities of this panel to resolve. But the panel members do believe that its persistence and the low priority given to the issue relative to other DOE scientific goals is indicative of the institutional attitude that DOE has had toward security: nonscientists have a poor understanding of all things nuclear, so their judgments about acceptable levels of risk are suspect prima facie.

FOREIGN VISITORS AND ASSIGNMENTS PROGRAM

True to the tradition of international partnership molded by the experiences of the Manhattan Project, the weapons labs have remained a reservoir of the best international scientific talent. Recent examples abound: a supercomputing team from Oak Ridge National Lab, made up of three PRC citizens and a Hungarian, recently won the Gordon Bell Prize; a Bulgarian and a Canadian, both world-class scientists, are helping Lawrence Livermore National Lab solve problems in fluid dynamics; a Spanish scientist, also at Livermore, is collaborating with colleagues on laser propagation.

But for more than a decade, the increasing prominence of foreign visitors in the weapons labs has increased concern about security risks. The PFIAB panel found that as early as 1985, the DCI raised concerns about the foreign visitors' program with the Energy Secretary. A year later, researchers conducting internal DOE review could find only scant data on the number and composition of foreign nationals at the weapons labs. Although intelligence officials drafted suggestions for DOE's foreign visitor control program, PFIAB found little evidence of reform efforts until the tenure of Secretary Watkins.

A 1988 GAO report cited DOE for failing "to obtain timely and adequate information on for-eign visitors before allowing them access to the laboratories." The GAO found three cases where DOE allowed visitors with questionable backgrounds—possible foreign agents—access to the labs. In addition, the GAO found that about 10 percent of 637 visitors from sensitive countries were associated with foreign organizations suspected of conducting nuclear weapons activities but DOE did not request background data on them prior to their visit. DOE also had not conducted its own review of the visit and assignment program at the weapons labs despite the DOE requirement to conduct audits or reviews at a minimum of every five years. Moreover, GAO reported that few post–visit or host reports required by DOE Order 12402 were submitted within 30 days of the visitors' departure and some were never completed.[50]

The following year, DOE revised its foreign visitor policy and commissioned an external study on the extent and significance of the foreign visitor problem. DOE's effort to track and vet visitors, however, still lagged well behind the expansion of the visitor program, allowing foreigners with suspicious backgrounds to gain access to weapons facilities. A study pub-lished in June 1990 indicated DOE had a "crippling lack of essential data, most notably no centralized, retrievable listing of foreign national visitors to government facilities." [51]

By September, 1992, DOE had instituted Visitor Assignment Management System (VAMS) databases, used to track visitors and assignees requesting to visit DOE. The system, however, failed to provide links between the labs that could be used for CI analysis and cross-checking of prospective visitors. Moreover, labs frequently did not even use the database and failed to enter visitor information. Instead, each lab developed its own computer program independently.

Reviews of security determined that, despite an increase of more than 50 percent in foreign visits to the labs from the mid–1980s to the mid–1990s, DOE controls on foreign visitors actually weakened in two critical areas: screening for visitors that may pose security risks, and monitoring the content of discussions

that might touch on classified information.

In 1994, DOE headquarters delegated greater authority to approve nonsensitive country visitors to the laboratories, approving a partial exception for Los Alamos and Sandia National Laboratories to forego background checks to help "reduce costs and processing backlogs." This resulted in almost automatic approval of some foreign visitors and fewer background checks. The FBI and GAO subsequently found that "questionable visitors, including suspected foreign intelligence agents, had access to the laboratories without DOE and/or laboratory officials' advance knowledge of the visitors' backgrounds."[52]

Changes in records checks over the past decade also made it easier for individuals from sensitive countries to gain access to the laboratories. In 1988, for example, all visitors from Communist countries required records checks regardless of the purpose of the visit. By 1996, records checks were only required for visitors from sensitive countries who visited secure areas or discussed sensitive subjects.

An internal DOE task force in 1996 determined that the Department's definitions of sensitive topics were not specific enough to be useful. It directed the DOE office of intelligence to develop a new methodology for defining sensitive topics, but did not set a due date. The 1996 group also called for a Deputy Secretary–level review of foreign visits and assignments to be completed by June 1997. [53] The PFIAB panel found no evidence to suggest that these tasks were accomplished.

In 1997, GAO found that DOE lacked clear criteria for identifying visits that involve sensitive subjects, U.S. scientists may have discussed sensitive subjects with foreign nationals without DOE's knowledge or approval; and the Department's counterintelligence program had failed to produce comprehensive threat assessments that would identify likely facilities, technologies, and programs targeted by foreign intelligence.a href="#54">[54] The study found that records checks were still not being conducted regularly on foreign visitors from sensitive countries. [55] Last year, 7,600 foreign scientists paid visits to the weapons labs.[56] Of that total, about 34 percent were from countries that are designated "sensitive" by the Department of Energy—meaning they represent a hostile intelligence threat. The GAO reported last year that foreign nationals had been allowed after-hours and unescorted access to buildings.[57]

Administration Track Records

CARTER
(Schlesinger: Aug '77-Aug '79; Duncan: Aug '79-Jan '81)

'77 DOE established ... First visiting U.S. scientists to China in '79 and '80 face Chinese elicitation effort. ...Late 1970s FBI investigates possible espionage at a lab. ...'80 GAO reports on problems safeguarding against the spread of nuclear weapons technology.

REAGAN I
(Edwards: Jan '81-Nov '82; Hodel: Nov '82-Feb '85; Herrington: Feb '85-)

'82 DOE's Inspection and Evaluation program formed ...GAO reports safeguards and security of weapons labs not adequate, recommends independent assessments program. ...'83 DOE issues threat guidance to provide a "consistent basis" for identifying vulnerabilities. ...Memo to DOE, DOD states President has "decided to strengthen WH role ... concerning the security of U.S. nuclear facilities."... President signs National Security Decision Directive (NSDD) on DOE security, ... DOE Safeguards and Security Steering Group formed at President's direction to oversee fulfillment of physical security improvements ... GAO reports security concerns at Rocky Flats facility, ... DOE conducts eight internal security inspections at weapons facilities and DOE HQ; provides criticisms and recommendations to DOE management. ... '84 DOE's Central Training Academy established for protective force personnel.

REAGAN II
(Herrington: Feb '85-Jan '89)

'86 Rep. Dingell letter to President re: lab security vulnerabilities, management problems and lack of confidence in DOE. ... Four GAO reports on DOE security and CI problems ... External report requested by DOE finds problems with management of foreign visitors and adequate security. ...'87 Three GAO reports on DOE highlight the transfer of technology to proliferating nations and inefficient security clearance program. ...Seven internal DOE security inspections criticize management and security practices in '87-'88. ...DOE initiates the Personnel Security Assurance Program (PSAP) ... DOE focuses on insider protection and strengthens classified document controls. ...Three DOE IG reports about security clearance problems from '86-'88. ...'88 Intelligence Community paper reflects concerns with international scientific exchanges at the DOE labs. ... President signs NSDD on Nuclear Weapons Safety, Security, and Control. ... FBI detailee

to DOE cites inaccessibility to senior DOE managers. ...President states "Improved nuclear security is an important legacy for us to leave the next administration;" DOE official opines that Energy has done "essentially all that can be done against the outsider threat." ... Senate Intelligence Committee staff briefed on CI activities at labs. ... Four GAO reports address DOE security and counterintelligence problems, including: major weaknesses in foreign visitor controls at labs, and foreign agents possibly gaining access to labs.

BUSH
(Watkins: Mar '89-Jan '93)

'89 New Secretary concerned about 1988 GAO criticism of DOE CI/security, defers DOE annual report on security until he reviews issue; NSC concurs. ... GAO finds insufficient control over weapons-related information and technology. ...'90 Four IG reports on security ... Secretary of Energy Advisory Board (SEAB) chartered ... Interagency CI group prepares assessment of intelligence threat to government facilities from visiting foreign nationals. ...GAO cites lack of clear, concise physical security standards and inconsistent material measurements at labs. ... Freeze Task Force critical of split management of classified and unclassified computer security; finds direction, coordination, conduct and oversight of safeguards and security activities throughout DOE warrant structural changes. ...External CI review highlights DOE's inability to manage comprehensive approach to foreign threat; inadequate oversight, control over secret document inventory; uncoordinated computer security responsibilities. ...'91 Four IG reports criticize security...GAO reports property, classified document control problems at LLNL; 10,000 documents unaccounted; inability of DOE to track, monitor, and correct security deficiencies ... '87, '89, and '91 GAO reports foreign countries routinely obtaining unclassified but sensitive information that could assist nuclear programs. ...Memo to President highlights previous security problems at DOE, Secretary's efforts to fix the deficiencies. ...'92 Two IG reports on security...SSCI-requested CI assessment finds DOE headquarters lacks authority to direct labs, CI resources, and current threat information. ...GAO cites weak internal security oversight controls; incomplete safeguards and security planning at DOE facilities. ...DOE Order on CI issued. ...DOE and FBI formalize relationship for conduct of CI activities. ...Internal security report to Secretary finds "personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements." ... Another report finds "Problems in management and oversight represent the most significant weakness" for the Department...and "security systems continue to be plagued with potential single point failures."

ENDNOTES

1. U.S. Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998.

2. Classified DOE Report.

3. Classified DOE Report.

4. Classified DOE Report.

5. Classified DOE Report.

6. DOE, Office of Counterintelligence, "The Foreign Intelligence Threat to Department of Energy Personnel, Facilities and Research, Summary Report," August 1990.

7. Classified U.S. Government report.

8. GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997.

9. Hewlett, Richard G. and Francis Duncan, "Atomic Shield: A History of the U.S. Atomic Energy Commission," May 1969.

10. Classified DOE report.

11. DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993

12. Classified FBI document.

13. Classified U.S. Government report.

14. Classified DOE report.

15. DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994 (U)

16. DOE/IG-385, "Special Audit Report on the Department of Energy's Arms and Military-Type Equipment," February 1, 1996

17. Classified DOE report.

18. DOE, "Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," September 1996

19. GAO/RCED-91-12, "Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities," October 1990 (U) and GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities," December 13, 1991

20. GAO/RCED-90-122, "Nuclear Security: DOE Oversight of Livermore's Property Management System is Inadequate," April 18, 1990

21. GAO/"Key Factors Underlying Security Problems at DOE Facilities," (Statement of Victor S. Rezendes, Director, Energy, Resources and Science Issues, Resources, Community, and Economic Development Division, GAO, in testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives), April 20, 1999

22. GAO/"Key Factors Underlying Security Problems at DOE Facilities," (Statement of Victor S. Rezendes, Director, Energy, Resources and Science Issues, Resources, Community, and Economic Development Division, GAO, in testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives), April 20, 1999

23. Classified DOE report.

24. Hewlett, Richard G. and Francis Duncan, "Atomic Shield, A History of the United States Atomic Energy Commission," May 1969

25. GAO/RCED-89-34, "Nuclear Security: DOE Actions to Improve the Personnel Clearance Program," November 9, 1988

26. DOE/IG/WR-O-90-02, "Nevada Operations Office Oversight of Management and Operating Contractor Security Clearances," March 1990;

27. Classified DOE report.

28. DOE/IG/WR-B-91-08, "Review of Contractor's Personnel Security Clearances at DOE Field Office, Albuquerque," September 1991.

29. DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993

30. DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1995," January 1996

31. Classified U.S. Government report.

32. Classified DOE report.

33. GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE Weapons Facilities," December 13, 1991.

34. Classified DOE report.

35. Classified DOE report.

36. DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994 (U)

37. DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1994," January 1995 (U)

38. Classified DOE report.

39. Classified DOE report.

40. Classified DOE report.

41. Classified DOE report.

42. Classified DOE report.

43. *New York Times*, "Abstract," August 5, 1977

44. DOE, "Plutonium: The First 50 Years. United States Plutonium Production, Acquisition, and Utilization from 1944 Through 1994

45. GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons

Facilities," December 13, 1991

46. GAO/RCED/AIMD-95-5, "Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking Capabilities are Limited," December 27, 1994

47. GAO/AIMD-95-165, "Department of Energy: Poor Management of Nuclear Materials Tracking Capabilities Are Limited," August 3, 1995

48. DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1995," January 1996

49. U.S. Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998

50. GAO/RCED-89-31, "Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories," October 11, 1988

51. Classified U.S. Goverment report.

52. GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997

53. Classified DOE report.

54. GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997

55. GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997

56. DOE, "Response to the Cox Committee Report: The Benefits of Department of Energy International Scientific and Technical Exchange Programs," April 1999.

57. GAO/RCED-99-19, "Department of Energy: Problems in DOE's Foreign Visitors Program Persist," October 6, 1998.

On to Next Section

Back to Report Top Page

FAS | **Secrecy** | **PFIAB Top Page** ||| **Index** | **Search** | **Join FAS**

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

ASSESSMENTS

RESPONSIBILITY

While cultural, structural, and historical problems have all figured into the management and security and counterintelligence failures of DOE, they should not be construed as an excuse for the deplorable irresponsibility within the agency, the pattern of inaction from those charged with implementation of policies, or the inconsistency of those in leadership positions. The panel identified numerous instances in which individuals were presented with glaring problems yet responded with foot–dragging, finger–pointing, bland reassurances, obfuscations, and even misrepresentations.

The record of inattention and "false start" reforms goes back to the beginning of DOE. There have been several Presidents; National Security Advisors, Energy Secretaries, Deputy Secretaries, Assistant Secretaries, and Lab Directors; scores of DOE Office Directors and Lab managers; and a multitude of Energy Department bureaucrats and Lab scientists who all must shoulder the responsibility and accountability.

As noted above, severe lapses in the security of the nation's most critical technology, data, and materials were manifest at the creation of the DOE more than 20 years ago. Many, if not most, of the problems were identified repeatedly. Still, reforms flagged amid a lack of discipline and accountability. The fact that virtually every one of those problems persisted—indeed, many of the problems still exist—indicates a lack of sufficient attention by every President, Energy Secretary, and Congress.

This determination is in no way a capitulation to the standard of "everyone is responsible, therefore no one is responsible." Quite the contrary. Even a casual reading of the open–source reports on the Department's problems presents one with a compelling narrative of incompetency that should have merited the aggressive action of the nation's leadership. Few transgressions could violate the national trust more than inattention to one's direct responsibility for controlling the technology of weapons of mass destruction.

The PFIAB panel was not empowered, nor was it charged, to make determinations of whether specific acts of espionage or malfeasance occurred regarding alleged security lapses at the weapons labs. Nor was it tasked to issue performance appraisals of the various Presidents, Energy Secretaries, or members of the Congressional leadership during their respective terms in office. However, an inquiry into the extent to which the system of administrative accountability and responsibility broke down at various times in history has been necessary to fulfill our charter. In fairness, we have tried to examine the nature of the security problems at DOE's weapons labs in many respects and at many levels, ranging from the

circumstances of individuals and the dynamics of group behavior to the effectiveness of mid–level management, the clarity of the laws and regulations affecting the Department, and the effectiveness of leadership initiatives.

THE RECORD OF THE CLINTON TEAM

To its credit, in the past two years the Clinton Administration has proposed and begun to implement some of the most far–reaching reforms in DOE's history. The 1998 Presidential Decision Directive on DOE counterintelligence (PDD-61) and Secretary Richardson's initiatives are both substantial and positive steps. We offer an analysis of some of these initiatives, and their likelihood of success, elsewhere in this chapter and elsewhere in this report.

However, the speed and sweep of the Administration's ongoing response does not absolve it of its responsibility in years past. At the outset of the Clinton Administration—in 1993, when it inherited responsibility for DOE and the glaring record of mismanagement of the weapons laboratories—the incoming leadership did not give the security and counterintelligence problems at the labs the priority and attention they warranted. It will be incumbent on the DOE transition team for the incoming administration in 2001 to pay particular heed to these issues.

While the track record of previous administrations' responses to DOE's problems is mixed (see box on previous administrations, on pp. 26-27), the panel members believe that the gravity of the security and counterintelligence mismanagement at the Department will, and should, overshadow post facto claims of due diligence by any administration—including the current one. Asserting that the degree of failure or success with DOE from one administration to the next is relative is, one might say, gilding a figleaf.

The fact is that each successive administration had more evidence of DOE's systemic failures in hand: the Reagan Administration arrived to find several years' worth of troubling evidence from the Carter, Ford, and Nixon years; the evidence had mounted higher by the time that the Bush Administration took over; and higher still when the Clinton Administration came in. The Clinton Administration has acted forcefully, but it took pressure from below and outside the Administration to get the attention of the leadership, and there is some evidence to raise questions about whether its actions came later than they should have, given the course of events that led the recent flurry of activity.

THE 1995 'WALK-IN' DOCUMENT

In 1995, a U.S. intelligence agency obtained information that has come to be called the "walk-in" document. A copy of a classified PRC report, it contains a discussion of various U.S. nuclear warheads. The PFIAB has carefully reviewed this document, related information, and the circumstances surrounding its delivery. Serious questions remain as to when it was written, why it was written, and why it was provided to the U.S. We need not resolve these questions. The document unquestionably contains some information that is still highly sensitive, including descriptions, in varying degrees of specificity, of technical characteristics of seven U.S. thermonuclear warheads. This information had been widely available within the U.S. nuclear weapons community, including the weapons labs, other parts of DOE, the Department of Defense, and private contractors, for more than a decade. For example, key technical information concerning the W–88 warhead had been available to numerous U.S. government and military entities since at least 1983 and could well have come from many organizations other than the weapons labs.

W-88 INVESTIGATION

Despite the disclosure of information concerning seven warheads, despite the potential that the source or

sources of these disclosures were other than the bomb designers at the national weapons labs, and despite the potential that the disclosures occurred as early as 1982, only one investigation was initiated. That investigation focused on only one warhead, the W–88, only one category of potential sources—bomb designers at the national labs—and on only a four-year window of opportunity. It should have been pursued in a more comprehensive manner. The allegations raised in the investigation should still be pursued vigorously. And the inquiry should be fully explored—regardless of the conclusions that may result.

The episode began as an administrative inquiry conducted by the DOE Office of Energy Intelligence, with limited assistance from the FBI. It developed into an FBI investigation, which is still under way today. Allegations concerning this case and related activities highlighted the need for improvements in the DOE's counterintelligence program, led along the way to the issuance of a Presidential Decision Directive revamping the DOE's counterintelligence program, formed a substantial part of the information underlying the Cox Committee's conclusions on nuclear weapons information, and ultimately led, at least in part, to the President's decision to ask this Board to evaluate security and counterintelligence at the DOE's weapons labs.

Clinton Administration Track Record

O'Leary: Jan '93–Jan '97

'93 New Secretary works to make labs more open...launches major declassification effort. ... DOE '92 Annual Report to President does not mention security problems highlighted same year in reports to Secretary .... GAO criticizes DOE's ineffective management of personnel security cases. ...Four IG reports on security...Internal report to Secretary on computer security uncovers lack of access controls; no configuration management; failure to perform management reviews. ...'94 Three IG reports on security...FBI detailees to DOE recalled because of "lack of control of the CI program by DOE HQ." ...Internal report finds classified and unclassified information on lab computer network. ...GAO reports computer security deficiencies found in 1985 at six facilities still not fixed. ...'95 Four IG reports on security...Congress considers numerous bills between '95–'99 to abolish DOE. ... "Galvin Task Force" offers SEAB options for change within the labs. ... "Walk-in" provides documents containing sensitive U.S. nuclear information. ...DOE officials meet with FBI regarding potential espionage involving nuclear weapons data. ...Analysis group formed at DOE to review Chinese weapons program; senior DOE, CIA, White House officials discuss options. ... GAO reports on poor management of nuclear material tracking capabilities ...Laboratory Operations (oversight) Board created. ...'96 First three lab-to-lab exchanges between U.S. and China. ...Internal DOE report discovers required nuclear material physical inventories not being performed. ...Two IG reports on security...DOE Deputy Secretary directs six "initiatives" to lab directors and field office heads for the foreign visitors and CI programs (most initiatives ignored after he leaves DOE in 1997.)

Pena: Mar '97–Jun '98

'97 Mar New Secretary confirmed. ... FBI report to Congress and DOE critical of DOE CI capabilities; addresses CI program oversight, foreign visits and assignments, CI analysis, professional training/CI awareness. ... FBI Director personally delivers CI review to Secretary. ...Two additional Lab-to-Lab exchanges held in Beijing. ...DOE staff briefs Congressional staff, and NSC, CIA, FBI senior officials on Chinese nuclear program, possible Chinese espionage before Secretary informed...DOE increases budget for CI in FY 1997, hires more CI professionals. ...Inter-agency Working Group reports that systemic and serious CI and security problems at DOE have been well documented over at least a ten year period ... few of the recommendations in the past studies have been implemented. ... A senior CI official states "There is every reason to believe the labs will resist" any outside assistance ... National Security Advisor requests independent assessment of China's nuclear program and the impact of U.S. nuclear information. ...Two DOE internal reports cite confusing, fragmented, dysfunctional security management structure. ...External report finds multiple, uncoordinated internal and external oversight activities. ...DCI and FBI Director meet with Secretary to discuss DOE CI problem and reform plan; ... meeting notes state "Despite all the studies conducted, experience over time has shown that DOE's structure and culture make reform difficult, if not

impossible, from within." ... Internal DOE report states "in all candor, we have been hampered in meeting [the safeguards and security] obligations by organizational obstacles and competing internal interests." ... PDD–61 drafted, coordinated in inter-agency process. ...DOE's Laboratory Operations Board finds "inefficiencies due to the Department's complicated management structure." ...Peter Lee (formerly of LLNL) pleads guilty, inter alia, to transmitting classified national defense information to representatives of the PRC in '85. ...GAO finds faulty procedures for foreign visitor indices checks and controlling dissemination of sensitive information; lack of clear criteria for identifying visits that involve sensitive subjects; indirect and inconsistent CI funding; DOE CI programs not based on comprehensive assessment of foreign espionage threat. ...Institute of Defense Analyses' "120 Day Report" finds inadequate management of DOE workforce and confusing chains of command. ...'98 Feb. President signs PDD-61. ...External report says DOE management and oversight of security problematic ...Security Management Board created by Congress, meets twice in next 18 months...CIA/FBI report provided to Congress on Chinese espionage activities. ... Jun 30 Secretary resigns, Deputy designated as Acting Secretary. ... DOE's 90-day report on CI reveals problems remain regarding separate management of classified and unclassified information. ...Lab-to-lab exchange held in Beijing.

Richardson: Aug '98 –
'98 Aug 18 New Secretary sworn in ...GAO again finds problems in DOE's foreign visitor program; notes lack of clear procedures for identifying sensitive subjects. ...External report highlights lack of DOE oversight expertise and ad hoc security structure. ... Per PDD–61, assessment of the foreign collection threat against DOE published. ...'99 DOE security review finds "unhealthy, adversarial environment of mistrust among DOE security organizations," recommends several management process changes ...Cox Committee publishes report...Lab-to-Lab exchange held in Beijing. ...President directs PFIAB to review security, CI at labs; directs Intelligence Community to conduct damage assessment of possible security breaches at labs; directs CI community to review security of nuclear weapons information in USG. ...DOE CI Implementation Plan delivered to Secretary. ...GAO reports inadequate separation of classified and unclassified computer networks at same lab in 1988, 1992, 1994, and 1998. ... "Chiles Report" describes management problems in nuclear weapons program. ...Internal DOE report highlights computer security problems at a lab. ... DOE counterintelligence implementation plan (per PDD–61) issued to labs. ... DOE shuts down all classified computers at LANL, LLNL, and SNL. ... DOE holds in-lab computer security conference. ... Secretary announces new security organization at DOE, to be headed by a "security czar."

It is not within the mandate of our review to solve the W–88 case or any other potential compromises of nuclear weapons information. Further, it is not within our mandate to conduct a comprehensive and conclusive evaluation of the handling of the W–88 investigation by the DOJ and FBI. In fact, as we understand it, that is the purpose of a task force recently appointed by the Attorney General. We trust that among the issues that the task force will resolve are:

- Whether the FBI committed sufficient resources, including agents with appropriate expertise, and demonstrated a sense of urgency commensurate with an apparent compromise of classified U.S. nuclear weapons information;
- Whether the DOJ Office of Intelligence Policy Review (OIPR) applied an inappropriately high standard to the FBI's request for electronic surveillance under the Foreign Intelligence Surveillance Act (FISA);
- Whether the FBI provided to DOJ OIPR all U.S. government information relevant to an appropriate

evaluation of the FBI's FISA request;

- Why the FBI's FISA request did not include a request to monitor or search the subject's workplace computer systems, particularly since an attorney in the FBI's General Counsel Office had provided an opinion in 1996 that such monitoring or searching in this case would require FISA authorization;
- Why the FBI did not learn until recently that in 1995 the subject had executed a series of waivers authorizing monitoring of his workplace computer systems;
- Whether the FBI adequately raised to the Attorney General the FBI's concerns over the declination of the FISA request;
- Whether communications regarding the subject's job tenure broke down between DOE, FBI, and Los Alamos.
- Whether the DOJ OIPR maintained appropriate records concerning FISA requests that were declined;
- Whether the FBI appropriately relied on technical opinions provided by the DOE;
- Why DOE, rather than the FBI, conducted the first polygraph examination in this case when the case was an open FBI investigation; and, perhaps most importantly,
- Whether additional cases should be opened to investigate whether the apparent disclosures may have arisen out of organizations other than Los Alamos lab.

Again, resolving these issues is not within our mandate. It is, however, explicitly within our mandate to identify additional steps that may need to be taken to address the security and counterintelligence threats to the weapons labs. Also, it is within our standing PFIAB obligation under Executive Order 12863 to assess the adequacy of counterintelligence activities beyond the labs. In this regard, what we have learned from our limited review of the W-88 case and other cases are significant lessons that extend well beyond these particular cases. These lessons relate directly to additional steps we believe must be taken to strengthen our safeguards against current security and foreign intelligence threats. Those steps are discussed further in the Classified Appendix to this report.

We have learned, for example, that under the current personnel security clearance system a person who is under FBI investigation for suspected counterintelligence activities may sometimes be granted a new or renewed clearance. We also have learned that although the written standards for granting a first clearance and for renewing an existing clearance may be identical, the actual practice that has developed—certainly within DOE and we strongly suspect elsewhere—is that clearance renewals will be granted on a lower standard. We find such inconsistency unacceptable. We think it appropriate for the National Security Council to review and resolve these issues.

We have also learned that the legal weapons designed to fight the counterintelligence battles of the 70s have not necessarily been rigorously adapted to fight the counterintelligence battles of the 90s (and beyond). For example, with the passage of more than twenty years since the enactment of the Foreign Intelligence Surveillance Act (FISA) of 1978, it may no longer be adequate to address the counterintelligence threats of the new millennium. We take no position on whether the statute itself needs to be changed. It may well still be sufficient. However, based on all of the information we have reviewed and the interviews we have conducted, and without expressing a view as to the appropriateness of the DOJ decision in the W–88 case, we do believe that the Department of Justice may be applying the FISA in a manner that is too restrictive, particularly in light of the evolution of a very sophisticated counterintelligence threat and the ongoing revolution in information systems. We also are concerned by the lack of uniform application across the government of various other investigative tools, such as employee waivers that grant officials appropriate authority to monitor sensitive government computer systems.

Moreover, there does not exist today a systematic process to ensure that the competing interests of law enforcement and national security are appropriately balanced. Law enforcement, rightly so, is committed

to building prosecutable cases. This goal is often furthered by leaving an espionage suspect in place to facilitate the gathering of more evidence. The national security interest, in contrast, is often furthered by immediately removing a suspect from access to sensitive information to avoid additional compromises. Striking the proper balance is never easy. It is made all the more difficult when there is no regular process to ensure that balance is struck. We have learned in our review that this difficult decision often is made by officials who either are too focused on the investigative details or are too unaware of the details to make a balanced decision. This is another matter deserving National Security Council attention.

PFIAB EVALUATION OF THE INTELLIGENCE COMMUNITY DAMAGE ASSESSMENT

Following receipt of the "walk-in" document, CIA, DOE, Congress, and others conducted numerous analyses in an effort to determine the extent of the classified nuclear weapons information the PRC has acquired and the resultant threat to U.S. national security. Opinions expressed in the media and elsewhere have ranged from one extreme to the other. On one end of the spectrum is the view that the Chinese have acquired very little classified information and can do little with it. On the other end is the view that the Chinese have nearly duplicated the W–88 warhead.

After reviewing the available intelligence and interviewing the major participants in many of these studies, we conclude that none of these extreme views holds water. For us, the most accurate assessment of China's acquisition of classified U.S. nuclear weapons information and the resultant threat to U.S. national security is presented in the April 1999 Intelligence Community Damage Assessment. Written by a team of experts, this assessment was reviewed and endorsed by an independent panel of national security and nuclear weapons specialists, chaired by Admiral David Jeremiah. We substantially agree with the assessment's analysis and endorse its key findings. The full text of the assessment's unclassified summary appears in the unclassified appendix.

PRESIDENTIAL DECISION DIRECTIVE 61: BIRTH AND INTENT

In mid–1997, it became clear to an increasingly broader range of senior administration officials that DOE's counterintelligence program was in serious trouble.[1] In late July, DOE officials briefed the President's National Security Advisor, who concluded that, while the real magnitude and national security implications of the suspected espionage needed closer scrutiny, there was nonetheless a solid basis for taking steps to strengthen counterintelli-gence measures at the labs. He requested an independent CIA assessment of China's nuclear program and the impact of U.S. nuclear information, and he directed that the National Counterintelligence Policy Board (NACIPB)[2] review the DOE counterintelligence program. That September, the National Security Advisor received the CIA assessment, and the NACIPB reported back that it had found "systemic and serious CI and security problems at DOE [had] been well documented over at least a ten year period" and "few of the recommendations in the past studies [had] been implemented." The NACIPB made 25 recommendations to significantly restructure the DOE CI program; it also proposed that a Presidential Decision Directive or Executive Order be handed down to effect these changes.

At an October 15 meeting, the Director of Central Intelligence and the FBI Director discussed with Secretary Pena and his Deputy Secretary the need to reform the DOE CI program. The DCI and FBI Director sought to make clear there was an urgent need to act immediately, and "despite all the studies conducted, experience over time [had] shown that DOE's structure and culture make reform difficult, if not impossible, from within." All agreed to develop an action plan that would serve as the basis for a Presidential Decision Directive. Several senior officials involved felt that the necessary reforms would—without the mandate of a Presidential directive—have little hope of overcoming the anticipated bureaucratic resistance, both at DOE headquarters and at the labs. There was a clear fear that, "if the

Secretary spoke, the bureaucracy wouldn't listen; if the President spoke, the bureaucracy might at least listen."

That winter, the NSC coordinated a draft PDD between and among the many agencies and departments involved. Serious disagreements arose over several issues, particularly the creation of independent reporting lines to the Secretary for the Intelligence and Counterintelligence Offices. Also at issue was the subordination of the CI officers at the labs. Much of the resistance stemmed simply from individuals interested in preserving their turf won in previous DOE bureaucratic battles. After much bureaucratic maneuvering and even vicious in–fighting, these issues were finally resolved, or so it seemed; and on February 11, 1998, the President signed and issued the directive as PDD-61.

The full PDD remains classified. An unclassified summary, which contains all significant provisions, is set forth in the unclassified annex. In our view, among the most significant of the 13 initiatives directed by PDD-61 are:

- The CI and foreign intelligence (FI) elements would be reconfigured into two independent offices and report directly to the Secretary of Energy;
- The Director of the new Office of CI (OCI) would be a senior executive from the FBI and would have direct access to the Secretary of Energy, the DCI and the Director of the FBI;
- Existing DOE contracts with the labs would be amended to include CI program goals and objectives and performance measures to evaluate compliance with these contractual obligations, and CI personnel assigned to the labs would have direct access to the lab directors and would concurrently report to the Director, OCI;
- The incoming Director, OCI would prepare a report for the Secretary of Energy ninety days after his arrival that would address progress on the initiative, a strategic plan for achieving long-term goals, and recommendations on whether and to what extent other organizational changes may be necessary to strengthen CI; and,
- Within 120 days, the Secretary of Energy would advise the Assistant to the President for National Security Affairs on the actions taken and specific remedies designed to implement this directive.

On April 1, 1998, a senior executive from the FBI assumed his duties as the Director of the OCI, and began his 90–day study. He completed and forwarded it to the Secretary of Energy on July 1, the day after Secretary Pena resigned. The Acting Secretary led a review of the study and its recommendations. On August 18, Secretary Richardson was sworn in. On November 13, he submitted the action plan required by the PDD to the National Security Advisor. Secretary Richardson continued to develop an implementation plan. The completed implementation plan was delivered to Secretary Richardson on February 3, 1999, and issued to the labs on March 4.

TIMELINESS OF PDD–61

Criticism has been raised that the PDD took too long to be issued and has taken too long to implement. Although the current National Security Advisor was briefed on counterintelligence concerns by DOE officials in April of 1996, we are not convinced that the briefing provided a sufficient basis to require initiation of a broad Presidential directive at that time. We are convinced, however, that the July 1997 briefing, which we are persuaded was much more comprehensive, was sufficient to warrant aggressive White House action. We believe that while the resulting PDD was developed and issued within a customary amount of time, these issues had such national security gravity that it should have been handled with more dispatch. That there were disagreements over various issues is not surprising; that the DOE bureaucracy dug in its heels so deeply in resisting clearly needed reform is very disturbing. In fact, we believe that the NACIPB, created by PDD in 1994, was a critical factor in ram–rodding the PDD through to signature. Before 1994, there was no real structure or effective process for handling these kinds of issues

in a methodical way. Had the new structure not been in place and working, we doubt if the PDD would have made it.

With regard to timeliness of implementation, we have far greater concern. It is not unreasonable to expect that senior DOE officials would require some time to evaluate the new OCI Director's 90–day study, and we are aware that Secretary Richardson did not assume his DOE duties until mid–August. However, we find unacceptable the more than four months that elapsed before DOE advised the National Security Advisor on the actions taken and specific remedies developed to implement the Presidential directive, particularly one so crucial.

More critically, we are disturbed by bureaucratic foot–dragging and even recalcitrance that ensued after issuance of the Presidential Decision Directive. Severe disagreements erupted over several issues, including whether the CI program would apply to all of the labs, not just the weapons labs, and the extent to which polygraph examinations would be used in the personnel security program. We understand that some DOE officials declined to assist in the implementation simply by declaring that, "It won't work." The polygraph program was finally accepted into the DOE's security reforms only after the National Security Advisor and the DCI personally interceded. The fact that the Secretary's implementation plan was not issued to the labs until more than a year after the PDD was issued tells us **DOE is still unconvinced of Presidential authority.** We find worrisome the reports of repeated and recent resistance by Office of Management and Budget officials to requests for funding to implement the counterintelligence reforms mandated by PDD-61. We find vexing the reports we heard of OMB budgeteers lecturing other government officials on the "unimportance" of counterintelligence at DOE.

SECRETARY RICHARDSON'S INITIATIVES

Since November of 1998 and especially since April of this year, Secretary Richardson has taken commendable steps to address DOE's security and counterintelligence deficiencies. In November of last year, in the action plan required by PDD-61, Secretary Richardson detailed 31 actions to be taken to reform DOE's counterintelligence program. These actions addressed the structure of the counterintelligence program, selection and training of field counterintelligence personnel, counterintelligence analysis, counterintelligence and security awareness, protections against potential "insider threats," computer security, and relationships with the FBI, the Central Intelligence Agency, and the National Security Agency.

Though many matters addressed in the action plan would require further evaluation before specific actions would be taken, immediate steps included granting to the Office of Counterintelligence (OCI) direct responsibility for programming and funding counterintelligence activities of all DOE field offices and laboratories; granting the Director, OCI the sole authority to propose candidates to serve as the counterintelligence officers at the weapons labs; and instituting a policy for a polygraph program for employees with access to sensitive information.

In April of 1999, in an effort to eliminate multiple reporting channels and improve lines of communications, direction and accountability, Secretary Richardson ordered changes in the department's management structure. In short, each of the 11 field offices reports to a Lead Program Secretarial Office (LPSO). The LPSO has "overall line accountability for site-wide environment, safety and health, for safeguards and security and for the implementation of policy promulgated by headquarters staff and support functions." A newly established Field Management Council is to be charged with program integration.

In May of 1999, Secretary Richardson announced substantial restructuring of the security apparatus at DOE. Among these is the new Office of Security and Emergency Operations, responsible for all

safeguards and security policy, cyber–security, and emergency functions throughout DOE. It will report directly to the Secretary and consist of the Office of the Chief Information Officer, and Office of Emergency Management and Response, and an Office of Security Affairs, which will include the Office of Safeguards and Security, the Office of Nuclear and National Security Information, the Office of Foreign Visits and Assignments, and the Office of Plutonium, Uranium, and Special Material Inventory.

Also announced was the creation of the Office of Independent Oversight and Performance Assurance. It also will report directly to the Secretary to provide independent oversight for safeguards and security, special nuclear materials accountability, and other related areas.

To support additional cyber-security improvements, DOE will be asking Congress for an additional $50 million over the next two years. Improvements are to include continual monitoring of DOE computers for unauthorized and improper use. New controls will also be placed on computers and workstations, removable media, removable drives, and other devices that could be used to download files. In addition, warning "banners" are now mandatory on all computer systems to alert users that these systems are subject to search and review at the government's discretion. Cyber–security training is also to be improved.

Secretary Richardson further announced additional measures designed to strengthen DOE's counterintelligence program. They include: a requirement that DOE officials responsible for maintaining personnel security clearances be notified of any information that might affect the issuance or maintenance of such a clearance, even when the information does not rise to the level of a criminal charge; and mandatory reporting by all DOE employees of any substantive contact with foreign nationals from sensitive countries. DOE also plans to strengthen its Security Management Board; accelerate actions necessary to correct deficiencies in security identified in the 1997/1998 Annual Report to the President on Safeguards and Security; expedite improvements in the physical security of DOE nuclear weapons sites; and delay the automatic declassification of documents more than 25 years old.

In sum, as of mid-June of 1999, progress has been made in addressing counterintelligence and security. Of note, all of the PDD–61 requirements are reported to have been substantially implemented. Other important steps also reportedly have been completed. Among these are the assignment of experienced counterintelligence officers to the weapons labs.

PROSPECTS FOR REFORMS

Although we applaud Secretary Richardson's initiative, we seriously doubt that his initiatives will achieve lasting success. Though certainly significant steps in the right direction, Secretary Richardson's initiatives have not yet solved the many problems. Significant objectives, all of which were identified in the DOE OCI study completed nearly a year ago, have not yet been fully achieved. Among these unmet objectives are revising the DOE policy on foreign visits and establishing an effective polygraph examination program for selected, high–risk programs. Moreover, the Richardson initiatives simply do not go far enough.

These moves have not yet accomplished some of the smallest fixes—despite huge levels of attention and Secretarial priority. Consider the following example: with all the emphasis of late on computer security, including a weeks–long stand–down of the weapons labs computer systems directed by the Secretary, the stark fact remains that, as of the date of this report, a nefarious employee can still download secret nuclear weapons information to a tape, put it in his or her pocket, and walk out the door. Money cannot really be the issue. The annual DOE budget is already $18 billion. There must be some other reason.

Under the Richardson plan, even if the new "Security Czar" is given complete authority over the more than $800 million ostensibly allocated each year to security of nuclear weapons-related functions in DOE, he will still have to cross borders into other people's fiefdoms, causing certain turmoil and infighting. If he

gets no direct budget authority, he will be left with little more than policy guidance. Even then, as the head of a staff office, under the most recent Secretary Richardson reorganization he has to get the approval of yet another fiefdom, the newly created Field Management Council, before he can issue policy guidance. Moreover, he is unlikely to have much success in obtaining approval from that body when he is not even a member—and the majority of those who are members are the very program managers that his policy guidance would affect.

TROUBLE AHEAD

Perhaps the most troubling aspect of the PFIAB's inquiry is the evidence that the lab bureaucracies— after months at the epicenter of an espionage scandal with serious implications for U.S. foreign policy—are still resisting reforms. Equally disconcerting, other agencies have joined the security skeptics list. In the past few weeks, officials from DOE and other agencies have reported to us:

- There is a heightened attention to security at the most senior levels of DOE and the labs, but at the mid–level tiers of management there has been lackluster response and "business as usual."
- Unclassified but sensitive computer networks at several weapons labs are still riddled with vulnerabilities.
- Buildings that do not meet DOE security standards are still being used for open storage of weapons parts.
- Foreign nationals—some from sensitive countries—residing outside a weapons lab have remote dial-up access to unclassified networks without any monitoring by the lab.
- In an area of a weapons lab frequented by foreign nationals, a safe containing restricted data was found unsecured. It had not been checked by guards since August 1998. When confronted with the violation, a mid–level official is said to have implied that it was not an actual security lapse because the lock had to be "jiggled" to open the safe door.
- A weapons lab was instructed to monitor its outgoing email for possible security lapses. The lab took the minimal action necessary; it began monitoring emails but did not monitor the files attached to emails.
- When Secretary Richardson ordered the recent computer stand-down, there was great resistance, and when it came time to decide if the labs' computers could be turned on again, a bevy of DOE officials fought to have final approval power.

BACK TO THE FUTURE

In 1976, federal officials conducted a study of the nation's nuclear weapons laboratories and plants. In trying to devise a coherent and viable way of managing the labs, they settled on three possible solutions: place the weapons labs under the Department of Defense, make them a free–standing agency, or leave them within the Energy Research and Development Administration. Congress chose to leave the weapons labs within ERDA, the successor agency of the Atomic Energy Commission.

Nearly a decade later, the oversight of the weapons labs was still of great concern. Senators Sam Nunn and John Warner led a push to place the weapons labs under the auspices of the Department of Defense. However, the Reagan Administration staved off their effort by agreeing to put together a blue–ribbon panel to study the issue. The panel studied the problem for six months and issued a report in July, 1985. Again, Congress and federal officials weighed whether the weapons labs should be transferred to the Department of Defense or restructured to be given more autonomy.

The status quo prevailed. The weapons labs stayed within the Department of Energy.

As this report has detailed, problems in the managerial relationship between DOE and the weapons labs

have persisted, perhaps even increased, over the past 14 years. Indeed, the discussion today sounds hauntingly familiar to the discussions in the 1980s and 1970s.

Today, however, there is a difference. The record of mismanagement of the weapons labs in matters of security and counterintelligence has become so long and so compelling as to demand a rejection of the status quo. There can be no doubt that the current structure of the Department of Energy has failed to give the nation's weapons laboratories the level of care and attention they warrant. Thus, our panel is recommending deep and lasting structural change that will give the weapons laboratories the accountability, clear lines of authority, and priority they deserve.

ENDNOTES

1. In April 1997, the FBI Director met with Secretary Pena, who had taken office in March, to deliver a highly critical FBI assessment of DOE's counterintelligence program. In June, DOE officials briefed the Special Assistant to the President and Senior Director for Nonproliferation and Export Controls. In July, the FBI Director and the Director of Central Intelligence expressed serious concern that DOE had not moved to implement the recommendations in the FBI report.

2. The National Counterintelligence Policy Board (NACIPB) was created by a 1994 Presidential Decision Directive to serve as the National Security Council's primary mechanism to develop an effective national counterintelligence program. Current core NACIPB members include senior representatives from the Director of Central Intelligence /Central Intelligence Agency, the Federal Bureau of Investigation, the Department of Defense, the Department of State, the Department of Justice, the military departments' CI organizations, the National Security Council, and, as of 1997, the Department of Energy and NSA.

On to Next Section

Back to Report Top Page

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

REORGANIZATION

What makes a government agency run well? There are a multitude of characteristics that arguably can make for an efficient and effective government agency or department. This Panel holds no illusions about the completeness of its understanding nor the purity of its wisdom regarding government bureaucracies. Indeed, some people would say that truly comprehending the inner workings of a federal department is the intellectual equivalent of grasping the enormity of the universe. Over the course of many years, however, we, as members of the President's Foreign Intelligence Advisory Board, have evaluated the performance of numerous federal entities, from the Department of Defense to the Foreign Broadcast Information Service. Some, we found, were in good order, others in pretty bad shape. In that sense, we believe we do know a lot about what makes some agencies work and not work. Although somewhat subjective and by no means exhaustive, our list of "good" things to look for includes several attributes.

LEADERSHIP

Certainly at the top, but also throughout the organization. The leaders and managers set the standards and expectations regarding performance and accountability. They are the foundation upon which a successful organizational culture is built. If management sets, demonstrates and enforces high standards for performance and accountability, there is a strong likelihood that the organization will follow. And, longevity is a key ingredient. For example, Daniel S. Goldin, Administrator of the National Aeronautics and Space Administration (NASA), was named to his post in the spring of 1992. Goldin has won considerable acclaim for demanding nothing but the best from his employees, and thereby turning around a bureaucracy that had become ossified and recalcitrant to higher authority, including the President. He did not do it overnight, though. His "watch" is now seven years long and still going. By contrast, the average stay for an Energy Secretary has been about two and a half years; a Deputy Secretary, less than two years; and an Under Secretary, less than 18 months.[1]

CLARITY OF MISSION

Employees must know who they are and why they are there. Mission statements may seem corny to some, but from our experience good ones work. NASA's is crisp, clear and bold: "NASA is an investment in America's future. As explorers, pioneers and innovators, we boldly expand frontiers in air and space to inspire and serve America, and to benefit the quality of life on Earth." The Energy Department also declares itself a department of the future; it's slogan is "Science, Security and Energy: Powering the 21st Century." However, we wonder if the DOE employees in the field really have a sense of purpose and

direction. Those at the Oakland Operations Office are challenged to, "serve the public by executing programs and performing DOE contract management." At Albuquerque Operations Office, the rallying cry is, "to contribute to the welfare of the nation by providing field-level federal management to assure effective, efficient, safe and secure accomplishment of the Department's national defense, environmental quality, science and technology, technology transfer and commercialization and national energy objectives."[2]

DEDICATION TO EXCELLENCE

It is the responsibility of leadership to emphasize continuously and top-to-bottom the absolute importance of quality of performance. People truly dedicated to excellence usually achieve it.

EMPHASIS ON CORE COMPETENCIES

Those agencies that constantly emphasize the business areas in which they must absolutely excel, usually do so. At NASA, we are told, rarely, if ever, does the Administrator give a speech in which safety is not emphasized. DOE has appropriately emphasized excellence in the quality of its scientific and technical work, but only recently has begun to emphasize security, and only in recent months has articulated the importance of counterintelligence. The panel was hard pressed to find either words mentioned in speeches by most of Secretary Richardson's predecessors.

MINIMAL POLITICAL PRESSURES

Blessed is the government manager whose operations fall into only a handful of Congressional districts and under the purview of only a couple of oversight committees. It doesn't take a nuclear scientist to understand that the more Congressional districts and committees with which a federal agency must contend, the more it is politically whip–sawed in its priorities and stuffed with pork. We suspect the Department of Energy probably holds some federal records: its multitudinous and widely cast operations come under the scrutiny of no less than 18 Congressional committees and fund well-paying federal and contractor jobs in more than 50 congressional districts.

STREAMLINED FIELD OPERATIONS

In just about any endeavor, but especially in managing government contracts, simpler is better. Managing government contracts has become a major function in more and more agencies and departments as they seek to cut costs. We know of a few good examples of agencies where this effort is both efficient and effective.

One is the National Reconnaissance Office (NRO), a semi-autonomous Defense Department agency, which has long managed huge contracts with major industrial firms that have built and help operate our nation's surveillance satellites. The NRO, however, came under heavy fire several years ago for budget irregularities, partly as a result of tangled lines of bureaucratic authority. Today, after some substantial streamlining, multi-million dollar contracts are run out of program management offices at NRO Headquarters on a line of accountability leading directly to the contracting company. Rather than maintaining large field offices, the NRO employs only a handful of representatives in the field—typically only one or two people resident at their largest contractors. The rest is done from Washington. To manage their largest contracts, no more than 15 contracting officers—from worker–level to management —are involved. Some are worth several billion dollars. Currently, the NRO manages over 1,000 contracts worldwide, with a combined value numbering in the tens of billions of dollars. They manage these contracts using a staff of approximately 250 contract officers.[3]

Though we acknowledge that there are differences between the missions of NRO's satellite contractors and DOE's nuclear weapons lab contractors, we are stunned by the huge numbers of DOE employees involved in overseeing a weapons lab contract. For example, Sandia National Weapons Laboratory, a contractor–operated facility in New Mexico, has several layers of Energy Department employees with whom it must deal: the Kirtland (Air Force Base) Area Office, with about 55 "feds," which is subordinate to the Albuquerque Field Office (AFO), which has a total complement of about 1,300 government workers. Albuquerque also monitors contracts with Los Alamos National Lab (through a Los Alamos Area Office of some 70 people), and several other contractors throughout the southern United States. Notably, Albuquerque is but one of 11 such DOE Field Offices, that boast a total field complement of about 6,000. Back at DOE Headquarters, which has a total work force of close to 5,000, Sandia's contracts are monitored, depending on the subject, by several Program Offices—including Defense Programs (somewhat over 100 officials) and Environmental Management (somewhat over 200 officials).

We repeatedly heard from officials at various levels of DOE and the weapons labs how this convoluted and bloated management structure has constantly transmitted confusing and often contradictory mandates to the labs. This is vividly illustrated by the labyrinthine organizational charts that one must decipher to trace lines of authority.

RESPONSIBILITY AND ACCOUNTABILITY IN SECURITY

One senior CIA official told us that the NRO security system is the best in the government—a view echoed, we understand, in a forthcoming report by the DCI/Defense Secretary Joint Security Commission. One can see why. At the NRO, security starts at the top. The chief of security provides policy guidance and monitors implementation. However, from the Director on down, all line managers are responsible for implementation. If a security breach occurs, the Director and appropriate line subordinates all are accountable. Similarly, NRO contractors are expected to meet fully NRO security standards and guidelines. Failure to meet those guidelines could well result in forfeiture of performance award fees, at the least.

FULL OPERATIONAL INTEGRATION

To be effective, security must be more than a concept, it must be woven into every aspect of the agency's business and the daily work of every employee. The NRO integrates security more fully than most other federal agencies we have seen. Though it has separate line items for security and counterintelligence functions, most security–related expenditures are integrated directly into the line items of every satellite program. Thus, rather than imposing security mandates as contract "add-ons," security officials work with the NRO managers to fold their requirements into a given program during the planning stages. In this structure, security requirements are as much a part of an NRO satellite program as are solar cells and thrusters. And, the NRO security professionals, rather than treated as staff functionaries, are accepted as true partners in the NRO mission.

A PREVAILING CONSCIOUSNESS

Making people aware is vital. The record clearly shows that DOE has had mixed results from its various security and counterintelligence indoctrination programs. Briefings, town hall meetings and educational films are helpful, but they cannot take the place of a working environment in which security is just part of the daily routine. Again at the NRO, when a management decision is made, security always gets a voice. A security official is present at every level of NRO decision making: from the Office Director, to his Board of Directors, to the management teams of the smallest NRO program, security officials are part of the management process. Moreover, "security" gets a vote equal to that of any program manager. From the record, we judge that security at DOE, until recently, only occasionally had a voice; and when it did, many

managers vociferously objected. Counterintelligence, on the other hand, was allowed little more than a whisper.

RESTRUCTURING

The panel is convinced that real and lasting security and counterintelligence reform at the weapons labs is simply unworkable within DOE's current structure and culture. To achieve the kind of protection that these sensitive labs must have, they and their functions must have their own autonomous operational structure free of all the other obligations imposed by DOE management. ***We strongly believe that this cleaving can best be achieved by constituting a new government agency that is far more mission–focused and bureaucratically streamlined than its antecedent, and devoted principally to nuclear weapons and national security matters.***

The agency can be constructed in one of two ways. It could remain an element of DOE but become semi-autonomous—by that we mean strictly segregated from the rest of the depart-ment. This would be accomplished by having the agency director report only to the Secretary of Energy. The agency directorship also could be "dual-hatted" as an Under Secretary, thereby investing it with extra bureaucratic clout both inside and outside the department.

We believe there are several good models for this course of action: the National Security Agency and the Defense Advanced Research Projects Agency, both elements of the Defense Department; and the National Oceanographic and Atmospheric Administration, an agency of the Commerce Department. Alternatively, the agency could be completely independent, with its administrator reporting directly to the President. The National Aeronautics and Space Administration and the National Science Foundation are also good models.

Regardless of the mold in which this agency is cast, it must have staffing and support functions that are autonomous from the remaining operations at DOE. These functions, which report directly to the Director, must include: an inspector general; a general counsel; a human resources staff; a comptroller; a senior official responsible solely for security policy, and another responsible solely for counterintelligence policy. To protect its autonomy and avoid the diversion of funds to other purposes, the agency budget must be a separate line item strictly segregated by Congress from other budget pressures—even if it remains nominally within the current DOE structure. The agency also must have a separate employee career service. The panel recommends an "excepted service" model of employment, like many of the intelligence community elements, which would facilitate accountability and higher performance levels by allowing management to reward, punish, hire, and fire employees more easily.

To ensure its long–term success, this new agency must be established by statute. That statute, moreover, must clearly stipulate that nothing less than an act of Congress can amend the agency's mission, functions or affiliations. Clearly, Congress and the President must decide definitively which of these two solutions to enact. The panel has no specific preference between them; we believe either can be made effective. Should Congress and the President conclude that retaining the agency inside DOE is not workable, the "wholly-independent" approach should be enacted.

We emphasize that it is very important for the new structure to be organized to preserve and, if possible, enhance the ability of the national weapons labs to attract and retain scientists of the highest caliber. Excellence in the caliber of the scientists and their research and development programs must be sustained if the weapons labs are to fulfill their missions in the front line of U.S. national security. To meet this goal, continued but carefully controlled interaction with foreign visitors and scientists from around the world as well as with researchers from DOE's nondefense labs is essential for producing the best science. In the semi-autonomous model, the Secretary would be responsible for managing and ensuring the effectiveness

of agency relations with the nonweapons labs.

Whichever solution Congress enacts, we do feel strongly that the new agency never should be subordinated to the Defense Department. Defense already is populated with a number of semi–autonomous agencies; we see no reason to add to that burden. Moreover, we believe the decision made long ago to house America's nuclear weapons research and development in a civilian government agency still makes sense. ***Specifically, we recommend that the Congress pass and the President sign legislation that:***

- ***Creates a new, semi–autonomous Agency for Nuclear Stewardship (ANS), whose Director will report directly to the Secretary of Energy.*** The Director should be dual–hatted as an Under Secretary of Energy. This new agency will oversee all nuclear weapons–related matters previously housed in DOE, including Defense Programs and Nuclear Nonproliferation; it also will oversee all functions of the National Weapons labs. (If Congress opts to create a totally independent agency, the Director should report directly to the President.)

- ***Streamlines the ANS/Weapons Lab management structure by abolishing ties between the weapons labs and all DOE regional, field and site offices, and all contractor intermediaries.*** The so–called "GOCO," or "government owned, contractor operated," concept of lab management should be retained. GOCO has been very successful, particularly in providing employment conditions that attract scientists of the highest caliber, and the federal government is strongly committed to maintaining that working relationship. Even if DOE opts to retain these field entities for other purposes, the ANS should sever all association with them. All ANS/Weapons Lab communications and business should be handled by ANS Liaison Offices established in each lab and manned with a small staff. (Our short review time did not permit us to explore fully this issue. We doubt that any amount of time would be sufficient. Suffice it to say that we did learn enough about the costs and benefits of these myriad DOE field bureaucracies to persuade us to recommend cutting all ties between them and the new agency.)

- ***Mandates that the Director/ANS be appointed by the President with the consent of the Senate*** and, ideally, have an extensive background in national security, organizational management, and appropriate technical fields. Admittedly, finding an individual with solid credentials in all three areas may prove an elusive goal. However, meeting two out of those three criteria should be considered mandatory, provided that one of the criteria always met is management experience. The Deputy Director should have a background in an area that compensates for areas in which the Director lacks experience. The Director should serve for a minimum fixed term of 5 years, not coincident with quadrennial transitions of administrations, and be subject to removal only by Presidential direction.

- ***Stems the historical "revolving door" and management expertise problems at DOE*** by severely circumscribing the number of political appointees assigned to ANS and requiring all ANS senior political appointees to have strong backgrounds in both national security (intelligence, defense, or foreign policy) and management (corporate, government, or military).

- ***Ensures effective administration of safeguards, security, and counterintelligence at all the weapons labs and plants by creating a coherent security/CI structure within the new agency.*** We strongly recommend following the NRO's model of security management. The senior CI official at ANS—we recommend a Special Assistant to the Director for CI policy—should be mandated as a permanent FBI senior executive service position.

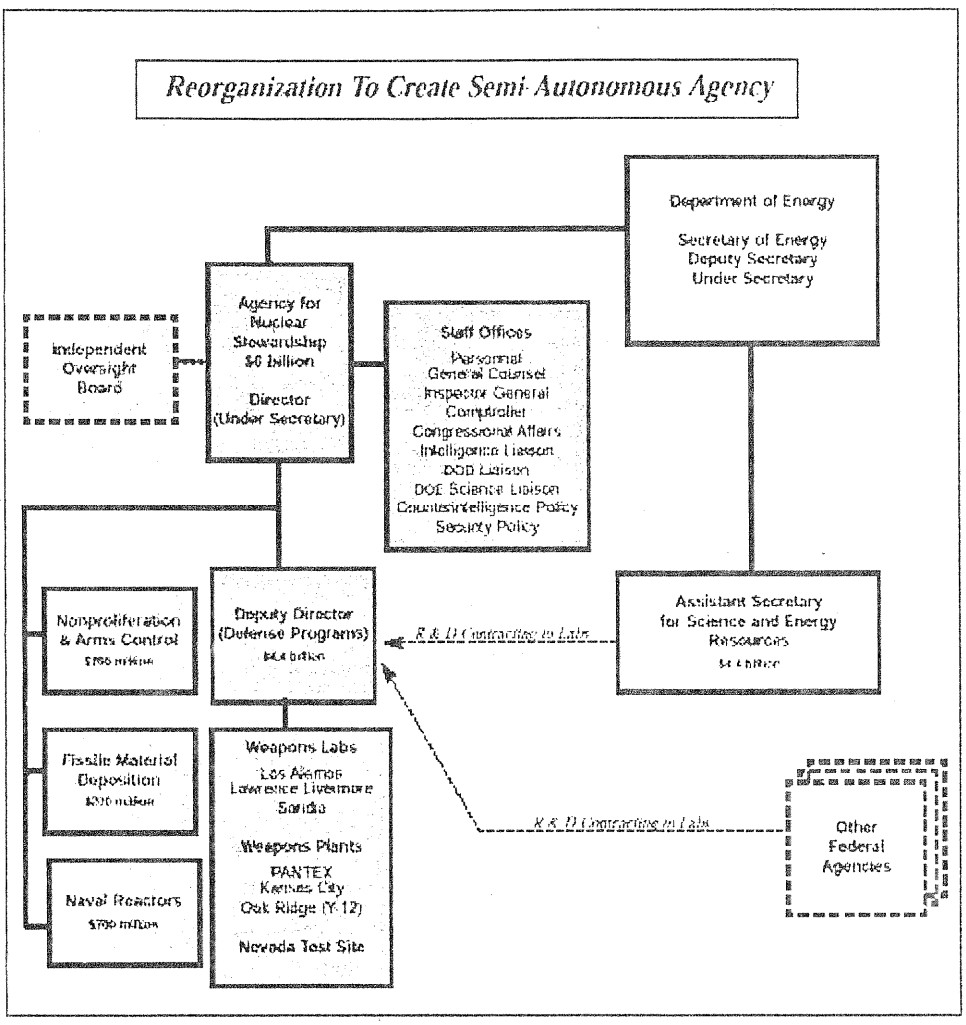
- ***Abolishes the Office of Energy Intelligence.*** A Special Assistant to the ANS Director for Intelligence Liaison should be created within the new agency, with a staff of no more than 20. The

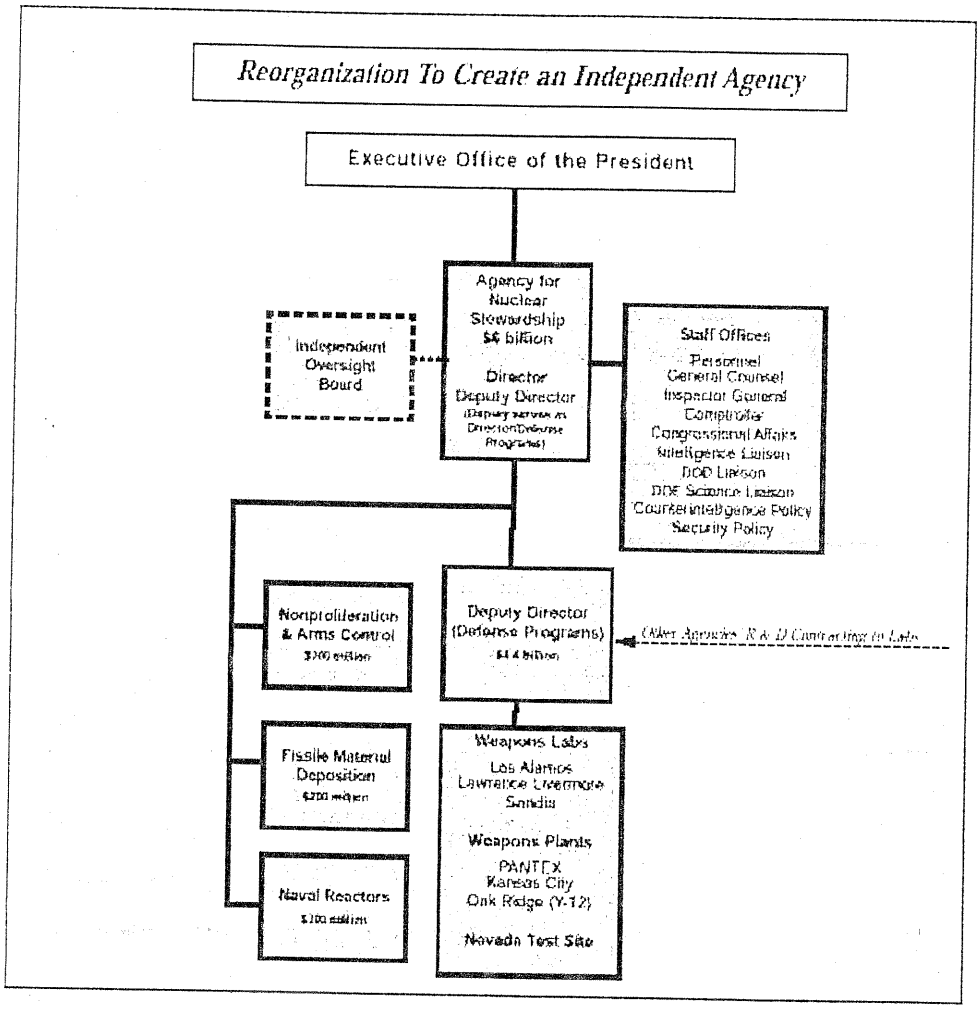
Special Assistant should be responsible for managing relations with the intelligence community, briefing ANS senior management on intelligence matters, and ensuring ANS intelligence requirements are met. This office should follow the Treasury Department model. (The Secretary of Energy would not be precluded from establishing a similar special assistant to address the department's non-weapons–related intelligence coordination and briefing needs.)

- Shifts the balance of analytic billets from the former Office of Energy Intelligence (about 40) to the DCI's Nonproliferation Center to bolster intelligence community technical expertise on nuclear matters. These billets should be permanently funded by ANS, but permanently assigned to the DCI Center. Weapons lab employees and ANS civil servants should be temporarily assigned to these positions for two year tours.

A Semi-Autonomous or Wholly Independent Nuclear Weapons Stewardship Agency should have the following attributes:

- The agency would be entirely separated from DOE, except in the semi-autonomous case, where the agency director—as a DOE Under Secretary—would report directly to the Secretary.
- The agency would have no other bureaucratic ties to DOE, other than R&D contracting, which would be managed by the agency Deputy Director. The weapons labs would be encouraged nonetheless to foster strong scientific interactions with the other DOE research labs. In the case of a wholly independent agency, the Director would be the chief executive officer.
- In the case of a semi-autonomous agency, the Director would be dual-hatted as a DOE Under Secretary.
- An independent oversight board would monitor performance and compliance to agency policies and guidelines, up and down the organizational structure.
- Authority from the agency Director to the weapons labs would run directly through the Deputy Director, who also would be dual-hatted as the Defense Programs Manager and, therefore, a manager of lab work.
- The security chief, directly reporting to the agency Director, would promulgate all security policies and guidelines for the agency and the weapons labs, including safeguards and cyber-security.
- The counterintelligence chief, also directly attached to the agency Director, would promulgate all counterintelligence policies and guidelines for the agency and the weapons labs. He/she also would manage the foreign visitors and assignments pro-gram.
- As Defense Programs Manager for the weapons labs, the agency Deputy Director would be responsible for ensuring the integration of all security and counterintelligence policies and guidelines into all weapons lab programs.
- Security officers and counterintelligence officers would be attached to all line offices, with heavy representation in Defense Programs, where full integration would occur. They also would be attached to all labs, in multiple numbers.
- Security and counterintelligence officers would report to their appropriate line managers on a day-to-day basis, but also report respectively to the agency security and counterintelligence chiefs on policy implementation issues. All policy implementation disputes would be referred back to the agency director for resolution.


Reorganization To Create Semi-Autonomous Agency
Department of Energy
Secretary of Energy
Deputy Secretary
Under Secretary
Independent Oversight Board
Agency for Nuclear Stewardship
$0 billion
Director (Under Secretary)
Staff Offices
Personnel
General Counsel
Inspector General
Comptroller
Congressional Affairs
Intelligence Liaison
DOD Liaison
DOE Science Liaison
Counterintelligence Policy
Security Policy
Nonproliferation & Arms Control
Deputy Director (Defense Programs)
Assistant Secretary for Science and Energy Resources
Fissile Material Disposition
Weapons Labs
Los Alamos
Lawrence Livermore
Sandia
Weapons Plants
PANTEX
Kansas City
Oak Ridge (Y-12)
Nevada Test Site
Naval Reactors
$790 million
Other Federal Agencies



ENDNOTES

1. DOE, "Department of Energy First Tier Organizations, Terms of Office, undated.

2. DOE, Field Fact Book, May 1998.

3. Unclassified organizational data provided by National Reconnaissance Office.

On to Next Section

Back to Report Top Page

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the
U.S. Department of Energy

ADDITIONAL RECOMMENDATIONS

There are a number of initiatives that must be undertaken immediately to start building a new agency culture and identity and restoring public confidence:

- Establish a clear mission and clear standards of excellence. The agency's mission, and that each subordinate unit, must be clearly articulated. Strong security and counterintelligence in addition to scientific achievement must be core elements of the mission. Similarly, clear standards of excellence must be established throughout the organization. Excellence must be the goal of scientists, engineers, technicians, and managers as well as security and counterintelligence officials.

- Establish a clear chain of accountability. There must be clear, simple, indelible lines of accountability from top to bottom. If a failure occurs, there must be a straightforward means for determining accountability—at all levels. Seeking consensus and advice is important, but ultimately a decision must be made by individuals, and those individuals should be held accountable.

- Hold leaders accountable. Accountability must be enforced, particularly among the agency managers who will form the backbone of the new agency and instill a new culture of excellence.

- Reward achievement. Criteria should be clear and rewards substantial. Protection of nuclear secrets and expansion of scientific knowledge should be among the most valued. Achievement must be judged on contribution to mission, not to program expansions or budget increases.

- Punish failure ... with severity, if necessary. Penalties should be tough, but fair and proportional. Laxity in protecting nuclear secrets and other sensitive information should be among the most severely punished.

- Train and educate. Establish a formal educational and training system to develop a professional cadre of career managers and leaders. Security and counterintelligence should be major parts of the core curriculum passed down to all lab personnel in regular briefings and training sessions.

- Do not forget the primary mission. Preserve and strengthen those agency attributes—including cutting edge research in the most advanced scientific fields—that will attract the finest talent in the nation. With respect to the weapons laboratories, continue to foster their unparalleled lead in intellectual excellence. But never lose sight that protecting the nation by securing its nuclear stockpile and nuclear secrets—through good science and good management—is Job Number One.

- While maintaining its autonomy, the agency should nonetheless emphasize continued close scientific interaction with the DOE research labs not engaged in weapons–related endeavors. In the semi–autonomous alternative, DOE should also be responsible for ensuring that good relations are maintained between the non-weapons labs and the weapons labs.

SECURITY AND COUNTERINTELLIGENCE ACCOUNTABILITY

- Accountability. The agency director should issue clear security accountability guidelines. The agency security chief must be accountable to the agency director for security policy at the labs, and the lab directors must be accountable to the agency director for compliance. The same system and process should be established to instill accountability among counterintelligence officials.

- Independent Oversight. Attentive, independent oversight will be critical to ensuring high standards of security and counterintelligence performance at the new agency. In that regard, we welcome Senator John Warner's recent legislative initiative to create a small, dedicated panel to oversee security and counterintelligence performance at the weapons labs. This oversight should include an annual certification process.

- Joint Committee for Congressional Oversight of ANS/Labs. Congress should abolish its current oversight system for the national weapons labs. Just as the profligate morass of DOE contractors and bureaucrats has frustrated the critical national interest of safeguarding our nuclear stockpile, so has the current scheme of Congressional oversight with roughly 15 competing committees laying claim to some piece of the nuclear weapons mission.

- ANS Inspector General. The President, Congress, and the director of the new agency should cooperatively, through executive order, legislation, and agency directive, provide teeth to the authority of the new agency's inspector general. For example, the inspector general, the independent oversight body, and the agency director should all have to concur on the findings of the annual report to the President on safeguards and security at the weapons labs.

EXTERNAL RELATIONS

- The CIA and FBI should expand their "National Security Partnership" to include the new agency and the weapons labs. Reciprocal assignment programs should be implemented to promote cross-fertilization of expertise and experience.

- CIA and DIA should bolster their support for ANS needs. Both intelligence agencies should establish analytic accounts to support the specific substantive and counterintelligence interests and needs of the new ANS and the weapons labs. These accounts, among other issues, should regularly produce data on the nuclear–related collection efforts of all foreign governments and foreign intelligence services. This data should serve as the foundation for regularized weapons lab counterintelligence briefs for the foreign visits/foreign visitors programs.

- Improve national security and law enforcement cooperation, particularly with respect to counterintelligence case referrals and handling. The National Security Council should take the lead in establishing clear Executive Branch guidelines and procedures for resolving disputes between agencies over law enforcement and national security concerns. A government–wide process needs to be established by which competing interests can be adjudicated by officials who are properly informed of all relevant facts and circumstances, but who also are sufficiently senior to make decisions stick.

- Ensure a government–wide review of legal tools to address the current foreign intelligence threat. The National Security Council should conduct a review to ensure that sufficient legal authority and techniques are available and appropriate in light of the evolution of a very sophisticated threat and the ongoing revolution in information systems.

PERSONNEL SECURITY

- An effective personnel security program. The agency director should immediately undertake a total revamping of the "Q" clearance program and look to the security elements in the intelligence community for advice and support. This review should result in a complete rewrite of existing guidance and standards for the issuing, revoking and suspending of security clearances. Special attention should be paid to establishing a clear—and relatively low—threshold for suspending clearances for cause, including pending criminal investigations. The review also should significantly strengthen the background investigation process by restructuring contracts to create incentives for thoroughness. We strongly advocate abolishing the prevalent method of paying investigators "by the case." Strict "need–to–have" regulations should be issued for regular reviews of all contract employees clearance requirements. Those without a continuing need should have their clearances withdrawn. The National Security Council should review and resolve issues on a government–wide basis that permit a person who is under FBI investigation for suspected espionage to obtain a new or renewed clearance; existing standards for clearance renewal also should be reviewed with an eye toward tightening up.

- A professional administrative inquiry process. Promulgate new agency guidelines and standards for security–related administrative inquiries to ensure that proper security/ counterintelligence procedures and methods are employed. Very high professional qualification standards should be established and strictly maintained for all security personnel involved in administrative inquiries.

PHYSICAL/TECHNICAL/CYBERSECURITY

- Comprehensive weapons lab cyber–security program. Under the sponsorship and specific guidance of the agency Director, the weapons labs should institute a broad and detailed program to protect all computer workstations, networks, links and related systems from all forms of potential compromise. This program, which should be reviewed by and coordinated with appropriate offices within the U.S. intelligence community, must include standard network monitoring tools and uniform configuration management practices. All lab computers and networks must be constantly monitored and inspected for possible compromise, preferably by an agency–sponsored, independent auditing body. A "best practices" review should be conducted yearly by the appropriate agency security authority.

- Comprehensive classified document control system. Document controls for the most sensitive data of the weapons labs should be reinstituted by the agency Director. The program should be constantly monitored by a centralized agency authority to ensure compliance.

- A comprehensive classification review. The new agency, in coordination with the intelligence community, should promulgate new, concise, and precise classification guidance to define and ensure awareness of information and technologies that require protection. This guidance should clear up the widespread confusion over what is export–controlled information; what information, when joined with other data, becomes classified; and the differences between similarly named and seemingly boundless categories such as "unclassified controlled nuclear information" and "sensitive but unclassified nuclear information."

BUSINESS ISSUES

- Make security an integral part of doing business. Security compliance must be a major requirement in every agency contract with the weapons labs. Rather than a detailed list of tasks, the contract should make clear the security and counterintelligence standards by which the lab will be held accountable. It is the responsibility of the lab to develop the means to achieve those objectives. If a lab fails to conform to these standards and requirements, the agency should withhold performance award fees.

- Review the process for lab management contracts. If the agency director has reason to open the bidding for lab management contracts, we strongly recommend an intensive market research effort. Such an effort would help ensure that legitimate and competent bidders, with strong records for productive research and development, participate in the competition.

- Weapons labs foreign visitors program. This productive program should continue, but both the agency and the weapons labs, in concert, must ensure that secrets are protected. This means precise policy standards promulgated by the agency to ensure: the integrity of the secure areas and control over all foreign visitors and assignees; a clear demarcation between secure and open areas at the labs; strong enforcement of restrictions against sensitive foreign visitors and assignees having access to secure facilities; and sensible but firm guidelines for weapons lab employees' contacts with foreign visitors from sensitive countries. Exceptions should be made by the agency director on a case–by–case basis. Clear, detailed standards should be enforced to determine whether foreign visits and appointments receive approval. The burden of proof should be placed on the employees who propose to host visitors from sensitive countries. Visits should be monitored by the labs and audited by an independent office. The bottom line: treat foreign visitors and assignees with the utmost courtesy, but assume they may well be collecting information for other governments.

- Foreign travel notification. The agency should institute a program whereby all agency and weapons lab employees in designated sensitive positions must make written notification of official and personal foreign travel well before departure. The agency must keep close records of these notifications and also ensure that effective counterintelligence briefings are provided to all such travelers. Unless formally granted an exception, scientists for weapons labs should travel in pairs on official visits to sensitive countries.

- Counterintelligence. The FBI should explore the possibility of expanding foreign counterintelligence resources in its field offices nearby the weapons labs. The panel offers additional thoughts for improving the Department's CI efforts in the Classified Appendix to this report.

On to Appendix

Return to Report Top Page

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

DOE COUNTERINTELLIGENCE AND SECURITY CHRONOLOGY

1976

U.S. Government assesses that China may step up efforts to acquire relevant nuclear technology.

1977

Department of Energy established, from the Energy Research and Development Administration, Federal Energy Administration, and elements of several Cabinet Departments.

May: Classified GAO report cites the need for an independent group to assess the adequacy of safeguards for nuclear material, and to assure the health and safety of the public from nuclear operations. In response to this and to DOE Inspector General reports, the Assistant Secretary for Defense Programs establishes an independent, inter-agency group to report to him on the adequacy of safeguards at weapons labs. The group finds that safeguards at sensitive facilities are not effective, while DOE's Office of Safeguards and Security was giving these facilities passing grades.

August: James R. Schlesinger becomes Secretary of Energy.

1979

Travel to PRC begins by U.S. persons associated with U.S. nuclear weapons program; travelers face Chinese elicitation efforts.

January 1: U.S. normalizes relationship with China.

August: DOE Secretary Schlesinger leaves office. Charles W. Duncan Jr. becomes new DOE Secretary.

September 21: GAO produces "DOE's Erroneous Declassification of Nuclear Weapons Design Document."

1980s

FBI completes espionage investigation begun in late 1970s. Case is not prosecuted because suspect and foreign agent do not confess.

1980

March 18: GAO produces, "Nuclear Fuel Reprocessing and the Problem of Safeguarding Against the Spread of Nuclear Weapons."

October 16: China conducts last atmospheric nuclear test.

1981

January: DOE Secretary Duncan leaves office. James B. Edwards becomes new DOE Secretary.

1982

DOE's Inspection and Evaluation program initiated. Program designed to focus on specific elements of a given protection program and consists of three distinct phases—interviews, evaluations and testing. Program results to be reported to the responsible Assistant Secretary and the Secretary.

August 20: GAO, in classified report, strongly recommends the reinstitution of a high-level group independently reporting to the Under Secretary on the state of safeguards at DOE.

November: DOE Secretary Edwards leaves office. Donald Paul Hodel appointed new Secretary of Energy.

1983

January 31: DOE issues classified policy statement characterizing potential threats to DOE facilities. DOE indicates, "this statement provides a consistent basis for the identification of vulnerabilities and the design of corrective actions at the Department's nuclear facilities."

July 8: President notifies Secretary of Defense and Secretary of Energy of his interest in strengthening the White House role in monitoring and overseeing programs concerning the security of U.S. nuclear weapons facilities. The Secretaries are instructed to provide quarterly status reports on security improvement programs, and any reports required by Congress, to the NSC.

1984

April 24: DOD publishes "Nuclear Weapon Systems in China," which estimates that the Chinese will not try to match the two superpowers in terms of nuclear capabilities, but will continue to seek Western technology support for their underground nuclear test program.

May: DOE establishes Central Training Academy to provide courses for protective force personnel in "tactical response, hostage negotiations, crisis management, and protective force supervisory skills." DOE designates Office of Safeguards and Security (OSS) as the single focal point for safeguards and security matters in DOE (residing in Defense Programs). The Office of Security and Quality Assessments is created, also reporting directly to the Assistant Secretary for Defense Programs.

July 2: In the Annual Report on Domestic Safeguards for 1983, DOE states that despite "improvements and initiatives" to the physical security program, "significant protection problems remain at many DOE facilities." DOE believes that the potential threat currently posed by the insider is serious and requires the institution of additional controls and personnel reliability features at our facilities."

1985

February: DOE Secretary Hodel leaves office. John S. Herrington becomes new Secretary.

June: DOE annual report to the President for 1984 states "Notwithstanding the progress that has been made [regarding major physical security construction projects], protection problems remain at a number of our nuclear facilities."

August: DCI plans to meet with Secretary of Energy to discuss controls on foreign nationals' access to the U.S. national laboratories.

September 13: DOE draft position paper on foreign visitor controls states it is clear that DOE has a "problem with foreign visitors and the control/regulation of them."

1986

Unpublished U.S. Government report discusses Chinese efforts to obtain U.S. nuclear information.

January 28: Representative John Dingell, Chairman of the House Energy and Commerce Subcommittee on Oversight and Investigations, sends letter to President Reagan regarding security vulnerabilities at the weapons laboratories. Rep. Dingell highlights additional management problems at DOE and the labs, and a lack of confidence in the inspection and evaluation function at DOE.

May 1: GAO produces report, "DOE Has Insufficient Control Over Nuclear Technology Exports."

1987

March 10: GAO produces report, "DOE's Reinvestigations of Employees Have Not Been Timely." (DOE was unable to eliminate the case backlog until 1993).

May: DOE's Inspector General reports a defective background investigative process at DOE.

June: DOE's Office of Security Evaluations finds several personnel security process errors at three DOE facilities.

August 17: GAO produces report, "Nuclear Nonproliferation: Department of Energy Needs Tighter Controls over Reprocessing Information."

December 29: GAO produces report, "DOE Needs a More Accurate and Efficient Security Clearance Program."

1988

April: DOE's Inspector General finds lack of accountability and insufficient timeliness in processing security clearances.

April 4: Minutes from a counterintelligence staff meeting, chaired by FBI Director, include an observation that "a significant problem we have had is that there were no real controls or focal points for tracking scientific visitors to China. Another problem was that academicians were rather naïve in their understanding of Chinese intentions, and it became very important to ensure that they were given a defensive CI briefing."

June: DOE's annual report to the President for 1987 comments, "As stated last year, DOE continues to be concerned about the potential threats posed by an insider, a knowledgeable and trusted individual who has been granted access to classified information or sensitive facilities. The threat posed by insiders is potentially more difficult to address than that of outsiders."

June 27: President signs and issues National Security Decision Directive 309, "Nuclear Weapons Safety, Security, and Control," tasking DOE and DOD to "determine the adequacy and effectiveness of physical security measures and coordinate their efforts including exchange of technical and operating data." DOE shall prepare an Annual Report on Nuclear Weapons Domestic Safeguards and Security ... that shall describe the current state of protection of all DOE domestic nuclear weapons facilities." The President further directs that he should be briefed on these reports annually.

October 1 1988 - August 8, 1989: FBI assigns official to DOE to evaluate CI program and to provide advice to DOE. FBI official found DOE management above the Counterintelligence Division inaccessible "which prevented him from securing the approval for the direct communication of urgently needed guidance to the field for the implementation of a vibrant counterintelligence program."

October 11: At a meeting, a DOE official briefs on the diverse nature of the security problems and the physical measures taken at the various Energy facilities which differ both technically and geographically. The official expresses the opinion that Energy had done "essentially all that can be done against the outsider threat."

October 11: GAO produces report, "Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories."

November: Senate Select Committee on Intelligence (SSCI) staff briefed on DOE's counterintelligence activities.

November 9: GAO produces report, "DOE Actions to Improve the Personnel Clearance Program."

December 12: Army CI officer provides a briefing to the interagency counterintelligence group on a GAO audit, "U.S. and Foreign Participation in R&D at Federal Laboratories." The GAO investigation concludes that most laboratories do not perceive the foreign presence as a problem.

1989

January: DOE Secretary Herrington leaves office.

March: James D. Watkins becomes new Secretary of Energy.

May: Secretary of Energy delays the annual security report to the President because he personally wants to assure himself of the adequacy of security measures.

June: GAO produces report, "Nuclear Nonproliferation: Better Controls Needed over Weapons-Related Information and Technology."

1990

January: Secretary of Energy Advisory Board (SEAB) is chartered as the highest level external advisory board in DOE. The SEAB reports directly to the Secretary. SEAB members form subcommittees and task forces to report on various issues for the Secretary.

April: DOE provides "1989 Annual Report to the President on Safeguards and Security." The report states that "ensuring proper and cost-effective protection of DOE domestic nuclear weapons facilities is, and will continue to be, one of the highest priority efforts in the Department." Concurrently, the Department will continue to pursue courses of action to mitigate the "insider threat," optimize its internal oversight function related to protection of weapon facilities, and ensure a reasonable and proper balance between safety, environmental, and safeguards and security responsibilities."

April: GAO produces report, "Nuclear Security: DOE Oversight of Livermore's Property Management System is Inadequate." (The Annual Report to the President in 1991 refers, in part, to this report, stating that "it has been determined that the primary cause of the document control problem was the number of document control systems which operated independently at the laboratory.")

April 6: DOE Secretary Watkins removes intelligence function from Office of Defense Programs (DP) and creates Office of Intelligence (IN) as a separate departmental element.

May 13: DOE issues supplemental policy guidance on protection against the potential insider threat.

June: Interagency working group prepares a study of specific threats to U.S. Government facilities from visiting foreign nationals; finds several DOE CI deficiencies.

June: DCI plans to meet with the Secretary of Energy to discuss concerns about the general lack of counterintelligence awareness at DOE facilities around the country, and the slow progress toward improving DOE's CI programs.

October: GAO produces report, "Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities."

1991

February 8: GAO produces report, "Nuclear Security: Accountability for Livermore's Secret Classified Documents is Inadequate."

March 21: GAO produces report, "Nuclear Nonproliferation: DOE Needs Better Controls to Identify Contractors Having Foreign Interests."

May 16: GAO produces report, "Nuclear Security: Property Control Problems at DOE's Livermore Laboratory Continue."

June 1: DOE provides 1990 Annual Report to the President which states, in part, that "significant improvements must be made immediately in safeguards and security areas involving planning and

management, personnel security, and the accounting for classified parts."

July 5: GAO produces report, "DOE Original Classification Authority Has Been Improperly Delegated."

July 8: Report from Energy Secretary Watkins on Safeguards and Security at DOE Nuclear Weapons Facilities highlights previous security problems at DOE and efforts to fix the deficiencies. It also notes that the report is not on the safety of nuclear weapons but rather on the safeguarding of classified information and materials.

December 13: GAO produces report, "Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities."

1992

April: At request of SSCI in FY92 intelligence authorization act, a community report cites insufficient resources in CI program, understaffing of debriefing elements, and lack of current threat information.

June: GAO produces report, "Nuclear Security: Weak Internal Controls Hamper Oversight of DOE's Security Problem."

October 30: GAO produces report, "Nuclear Security: Safeguards and Security Planning at DOE Facilities Incomplete."

October: DOE Order on counterintelligence issued.

October 7: DOE and FBI formalize relationship for conduct of CI activities in Memorandum of Understanding. MOU's purpose is to "define procedures that are mutually acceptable to the FBI and DOE regarding the conduct and coordination of counterintelligence activities and investigations involving DOE programs, facilities, or personnel in the United States."

November: DOE's Office of Security Evaluations' report for FY 1992 to the Secretary states, "Management and oversight problems ... continue to be the root cause of many other deficiencies noted in Security Evaluation inspections during FY 92;" and the "Department's Protection of Information programs suffer from lack of adequate guidance and a fragmented approach for protecting information."... "As noted in the past two reports, problems in management and oversight represent the most significant weakness in the Department's safeguards and security program." ... "Security systems continue to be plagued with potential single point failures and inadequate life cycle planning."

November 16: GAO produces report, "Nuclear Security: Improving Correction of Security Deficiencies at DOE's Weapons Facilities."

1993

January: DOE Secretary Watkins leaves office. Hazel R. O'Leary becomes new DOE Secretary.

February: The Annual Report to the Secretary on Safeguards and Security for 1992 finds that "less than satisfactory ratings in the area of classified matter protection and control stem in large part from the need for site management to assume responsibility for completion of self-assessments and

provide training for document control." Another security program "has suffered from a lack of management focus and inconsistent procedural execution throughout the DOE complex. The result is that personnel are seldom held responsible for their disregard, either intentional or unintentional, of security requirements."

April: In the Annual Report to the President for 1992, DOE states that there is "an extensive reorganization of the laboratory safeguards and security organization underway to more effectively and efficiently administer the laboratory program."

May 10: GAO produces report, "Efforts by DOD & DOE to Eliminate Duplicative Background Investigations."

August 12: GAO produces report, "DOE's Progress on Reducing Its Security Clearance Workload."

1994

January: The Annual Report to the Secretary on Safeguards and Security for 1993 states that there is "growing confusion within the Department with respect to Headquarters' guidance for safeguards and security. At this time, there is no single office at Headquarters responsible for the safeguards and security program. Most recently, a number of program offices have substantially expanded their safeguards and security staff to office-size organizations. These multiple safeguards and security offices have resulted in duplication of guidance, unnecessary requests for information/clarification, and inefficient program execution. Unchecked, this counterproductive tendency threatens the success of the overall safeguards and security effort."

March: FBI detailees to DOE are recalled to FBI "to address internal FBI needs," because of "lack of control of the CI program by DOE Headquarters [which] resulted in futile attempts to better manage the issue of foreign visitors at the laboratories."

April: The DOE Safeguards and Security Annual Report to the President for 1994 states that DOE's "safeguards and security community has begun to aggressively respond to the Secretary's goal of openness and public access to government information while recognizing the need to provide appropriate and effective security policy and procedures."

June: Intelligence report states Chinese visitors to U.S. are attempting to acquire U.S. technology through the recruitment of experts.

1995

January: The 1994 Annual Safeguards and Security Report to the Secretary finds that information security management programs "generally reflect deficiencies in self-inspection programs, control of access to classified and caveated information, and training regarding handling of classified information." Many findings regarding information security "are directly due to a lack of organizational and administrative detail on the part of those being inspected. Overall, findings and surveys, much like last year, continue to reflect deficiencies in self-inspections and procedural requirements or inappropriate or inadequate site guidance ... In the area of classified matter protection and control, like last year, marking, accountability, protection, and storage deficiencies are most numerous."

February: DOE Office of Counterintelligence subordinated to Office of Intelligence.

July: DOE senior officials discuss possibility that China may have classified U.S. nuclear design information with CIA, FBI and White House senior officials in several meetings this summer.

Summer: Analytical working group meets on China's nuclear weapons program and possible access to U.S. information. Group concludes that China has obtained classified U.S. information but disagrees on impact.

August 3: GAO produces report, "Poor Management of Nuclear Material Tracking Capabilities Makes Success Unlikely."

1996

January: DOE's annual safeguards and security report to the Secretary notes that among the disturbing trends in 1995 are "severe budget reductions, diminished technical resources, increased responsibilities, and reduced mission training, which have undermined protection of special nuclear material and restricted data." The report states that "continued budget cuts and diminishing resources have reduced protection program operations to a level of 'single point failure.'" The report also reviews personnel security, and finds there are cases of "identified individuals who held security clearances for convenience only." Problems are "symptomatic of the lack of management attention to basic information assurance concerns."

January 23-27: China Arms Control Exchange (lab-to-lab) Workshops: CTBT Verification and Monitoring Technologies, and Nuclear Materials, Protection, Control and Accounting (MPC&A), in Beijing.

March: DOE Deputy Secretary initiates study of foreign visits and assignments to labs.

March 25-29: China Arms Control Exchange (lab-to-lab) Workshop: Cooperative Monitoring Technologies, in Albuquerque.

April 13: DOE briefs Deputy National Security Advisor and senior NSC and CIA officials on "China's Nuclear Weapons Programs: Strategic Directions and Foreign Contributions."

May: DOE Administrative Inquiry is completed.

June 17-20: China Arms Control Exchange (lab-to-lab) Workshop: Atmospheric Sciences (#1), in Livermore, CA.

September: The 1995 Annual Report to the President (not forwarded to the White House until March 1997) is issued. Citing declining resources, DOE states that "many program elements have been reduced to minimally effective levels," and without "adequate investment, [and] senior level management support ... the nation's special nuclear material stockpile could be placed at increased risk and our international leadership in nuclear nonproliferation will be diluted." Increased use of computer systems for handling classified and sensitive unclassified information "increases the potential and probability for 'hacking' and for covert collection of information from unprotected or lightly protected systems." Simply stated, "Classified and sensitive unclassified information related to special nuclear materials and weapons production is increasingly at risk."

October: DOE Office of Counterintelligence expanded; CIA CI expert designated to run office.

October: Intelligence reports cite several foreign countries are actively seeking U.S. nuclear

information.

October 16: DOE's Office of Intelligence forwards a plan to better detect espionage through training and awareness briefings.

November 21: DOE Deputy Secretary meets with lab directors and heads of DOE field offices to review foreign visitors and CI programs. DOE HQ, field offices, and labs directed to begin implementing new measures to strengthen foreign visitor and CI programs. Labs tasked to produce threat self-assessment.

1997

January: The 1996 Annual Report on Safeguards and Security for the Secretary states, "Important security functions are operating under conditions of 'single-point failure.'" DOE's aging safeguards and security systems are cited as nearing the end of their useful lives, and "they no longer provide the necessary level of protection required in today's security environment."

March 12: Federico Pena confirmed as Secretary of Energy.

April 4: FBI issues report (in response to the FY97 Intelligence Authorization Act) to the Community Management Staff for transmittal to Congress and DOE. Report addresses: CI program oversight, foreign visits and assignments, CI analysis, professional training/CI awareness, and investigations.

April 7: FBI Director Freeh meets with Secretary of Energy Pena to deliver the April 4, 1997 report.

April 28: DOE Office of Intelligence organizes a Counterintelligence Senior Advisory Group to provide recommendations for DOE's CI problems.

June 19-29: China Arms Control Exchange (lab-to-lab) Workshop: Atmospheric Sciences (#2), in Beijing.

July 14: Briefing on possible espionage provided to Secretary of Energy with options for remedies.

July 29: DOE briefs National Security Council staff on "China's Strategic Nuclear Modernization Program: DOE Nuclear Weapons Laboratory Contributions to Chinese Strategic Breakthroughs."

August 6-8: China Arms Control Exchange (lab-to-lab) Workshop: Control of Nuclear Technologies, in Beijing.

August 12: At the conclusion of a DOE briefing on China's possible possession of U.S. warhead design information, FBI Director recommends that "DOE quickly and 'furiously' develop a plan to stop erosion of 20 years."

September 2: NACIPB/NACOB reports that the "working group has recognized that systemic and serious CI and security problems at DOE have been well documented over at least a ten year period. Information received from CI and security professionals at DOE indicate that few of the recommendations in the past studies have been implemented."

September 25: GAO produces report, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories."

October 15: DCI and FBI Director meet with Secretary of Energy and Deputy Secretary to discuss CI problems and reforms. Participants agree to develop action plan that will serve as basis for Presidential Decision Directive (PDD), acknowledging that reform from within DOE is difficult.

November 6: Letter to Secretary of Energy from DCI and FBI Director states "the culture and structure at DOE have consistently prevented meaningful reforms which could begin to counter the foreign intelligence threat to sensitive weapons programs and dual use technology."

November 6: DOE's Office of Security Affairs submits "Report on the Status of the Department of Energy's Safeguards and Security Program, October 1997" to the Secretary. The cover letter states, "in all candor, we have been hampered in meeting [safeguards and security] obligations by organizational obstacles and competing internal interests." The report contends that "by far, the most pressing issue is the Department's current unsatisfactory method for managing its safeguards and security program. Simply put, the current method does not work as intended."

1998

February 11: President signs PDD-61.

March: U.S. Nuclear Command and Control System (NCCS) Support Staff (NSS) produces assessment report on DOE Nuclear Weapons Related Security Oversight Process. The report finds that DOE's ability to "exercise comprehensive oversight, provide critical expert advice and status assessment to senior management, and identify corrective actions and monitor their implementation is problematic due to three significant issues: 1) a lack of nuclear physical security expertise at all levels of the oversight process; 2) ad hoc structuring of Safeguards and Security functions throughout the Department; and 3) placement of oversight functions in positions which constrain their effectiveness." DOE's initial response to the above list of findings was "without references to specific examples in the body of the report, these issues cannot be validated."

March: DCI and FBI Director meet with DOE lab directors to discuss the importance of the new initiatives.

April 6-May 15: DOE CI Director begins PDD-61-mandated 90-day study with team visits to eight DOE operations offices and nine national laboratories.

June 30: Secretary Pena resigns.

July 1: Acting Secretary receives 90-day report.

July: Joint Technology Demonstration (lab-to-lab Exchange), Nuclear Materials Protection, Control and Accounting (MPC&A), in Beijing.

August 18: Secretary Richardson sworn in.

October 6: GAO produces report, "Problems in DOE's Foreign Visitor Program Persist."

November: Per PDD-61, report published on the foreign collection threat to DOE, stating that DOE is being aggressively targeted for nuclear, sensitive, proprietary, and unclassified information.

November: During an internal inspection of a lab, DOE finds that the "underlying cause of these

security breaches has been personnel who lack adequate security awareness and training, and who do not demonstrate an attitude conducive to effective security."

November 13: Secretary Richardson submits CI Action Plan to NSC. December 9: Secretary Richardson meets with lab CI directors, and HQ CI and Intelligence staff to discuss implementation plan.

1999

January: First phase of a Special Security Review is completed for the Secretary. The recommendations include: establishing an integrated security management system; formalizing and differentiating the roles and responsibilities of each DOE organization; optimizing safeguards and security resources; strengthening human reliability programs; and incorporating security responsibilities into safety concerns.

January 3: U.S. House of Representatives publishes "Final Report of the Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China" (classified version).

January 25-30: Joint Technology Demonstration (lab-to-lab Exchange), Nuclear Materials Protection, Control and Accounting (MPC&A), in Beijing.

February 3: DOE's CI Implementation Plan completed and delivered to Secretary Richardson.

February 19: GAO produces report, "Concerns with DOE Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists."

March: DOE forwards the "annual" safeguards and security report from the past two years to the President, citing that there is "concern that attitudes regarding the protection of critical information are moving toward a less-attentive state of awareness."

March 4: DOE Counterintelligence implementation plan (per PDD-61) issued to labs.

April 6: DOE temporarily shuts down all classified computers at LANL, LLNL, and SNL for security review.

May 11: Secretary Richardson announces new security organization at DOE, under the responsibility of a "security czar."

On to Next Section

Back to Report Top Page

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

CHRONOLOGY OF SECURITY ANALYSIS REPORTS OF DOE, 1980-1999

PHYSICAL PROTECTION OF SENSITIVE NUCLEAR DATA, MATERIALS, AND TECHNOLOGY

Sep 1979

GAO/EMD-79-109/DOE's Erroneous Declassification of Nuclear Weapons Design. Los Alamos, sometime between 1971 and 1976 -- while under AEC, incorrectly declassified very sensitive weapons design information, which subsequently was found in publicly accessible library in Los Alamos.

Mar 1980

GAO/EMD-80-38/Nuclear Fuel Reprocessing and the Problems of Safeguarding Against the Spread of Nuclear Weapons. Improper measuring, storing, and verifying of quantities of nuclear materials.

Sep 1982

DOE/Office of Safeguards and Security (OSS) Inspection Report on Albuquerque Area Office, Los Alamos National Lab (LANL), Sandia National Lab (SNL), and Rocky Flats Plant. Classified findings

May 1984

DOE/Office of Safeguards and Quality (OSQ) Assessment: LANL, SNL, LLNL. Classified findings.

Jan 1985

DOE/OSQ Assessment: Inspection Report on Albuquerque Area Office, LANL, Mound Facility. Classified findings.

Feb 1985

DOE/OSQ Assessment: Inspection Report on DOE Germantown and Forrestal Locations. Classified findings.

Jun 1985

DOE/OSQ Assessment: Inspection Report on SNLL, LLNL, San Francisco Operations Office. Classified findings.

Jan 1986

U.S. House of Representatives: Letter of Rep. Dingell letter to the President. Inadequately trained guard force personnel; inadequate protection of classified information; inability to track and recover special nuclear material.

Nov 1986

DOE/OSQ Assessment: Inspection Report on LANL, Albuquerque Area Office. Classified findings.

Apr 1987

DOE/OSE: Inspection Report on San Francisco Operations Office and SNLL. Classified findings.

Aug 1987

GAO/RCED-87-150/DOE Needs Tighter Controls Over Reprocessing Information. Transfer of sensitive nuclear technology to proliferating nations. DOE funding of research that may involve foreign nationals from countries that have not agreed to Non-Proliferation Treaty.

Jun 1989

GAO/RCED-89-116/Nuclear Proliferation: Better Controls Needed Over Weapons-Related Information and Technology. Insufficient control over weapons-related information and technology.

Dec 1990

DOE Safeguards and Security Task Force/Freeze Report. Lack of clear and concise physical security standards; inconsistent measurements of nuclear material.

Aug 1991

DOE/IG-296/ Department-wide Audit of the Visibility Over the Status of Nuclear Materials. Nuclear materials routinely reported as "in use" or "needed" when they were actually "excess" to any defined requirement.

Dec 1991

GAO/RCED-92-39/Nuclear Security Safeguards and Security Weaknesses at DOE's Weapons Facilities. Noncompliance with two-person rule for access to nuclear material; physical security personnel unable to demonstrate basic skills.

May 1992

DOE/IG/INS-L-92-02/Control of Classified Documents at DOE Savannah River Operations Office. No review of Savannah River classified document controls by DOE Headquarters Office of Security Evaluations Between 1985 and 1990.

Jan 1993

DOE/IG-319/ Administration of Conflict of Interest Relating to Tech Transfer at LANL. Conflict of interest by LANL employees, who made decisions, used government resources, and took privileged information to further personal financial interest in spin-off business.

Feb 1993

DOE/OSS/ 1992 Annual Report to the Secretary. Aging equipment; lack of adequate system performance testing.

Aug 1994

DOE/IG/INS-O-94-05/Inspection of Physical Security Operations at LANL TA-18 Site. LANL not in full compliance with DOE physical security requirements because of LANL's failure to meet deadline for completion of site safeguards and security plan.

Jan 1995

DOE/OSS/Status of Safeguards and Security, Fiscal Year 1994. Numerous deficiencies in marking, accountability, protection, and storage of classified material.

Mar 1995

DOE/IG/S941S012/ Albuquerque Vault Classification. Inadequate procedures for protecting combinations to security containers/areas.

Jun 1995

DOE/Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. Aging security systems.

Jan 1996

DOE/OSS/Status of Safeguards and Security, Fiscal Year 1995. Aging security systems.

Sep 1996

DOE/Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. Aging safeguards and security systems and protective forces; inadequate inventory procedures for some facilities.

Jan 1997

DOE/OSS/Status of Safeguards and Security for 1996. Classified findings.

Nov 1997

DOE/OSA/Report to Secretary on Status of DOE Safeguards and Security Program. Aging physical security systems and protective force.

Jun 1997

SNL/Factors Contributing to Current Risk Levels in DOE Complex. Classified finding.

Apr 1999

DOE/23rd Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. Aging security systems.

Feb 1999

GAO/RCED-99-54/Concerns with DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists. DOE may have provided Russian scientists with dual-use, defense-related information that could negatively affect national security.

PERSONNEL SECURITY

Jul 1984

DOE/Ninth Annual Report on Domestic Safeguards. Classified findings.

Jul 1986

DOE/IG-228/Retention of Security Clearances at DOE Headquarters. Ineffective procedures for systematically withdrawing clearances after employee termination.

Mar 1987

GAO/RCED-87-72/DOE's Reinvestigation of Employees Has Not Been Timely. Personnel security reinvestigations not conducted on timely basis (DOE unable to eliminate case backlog until 1993).

May 1987

DOE/IG-238/Selected Aspects of DOE's Personnel Security Program. Employees granted clearances higher than required; majority of employees not reinvestigated in last 5 years; defective investigative process.

Jun 1987

DOE/OSE Inspection Report on Albuquerque Operations Office, LANL. AL and SNL. Lack of procedure to establish eligibility requirement for SCI clearance if family member non-US citizen; lack of timely conduct and analysis of reinvestigations; Albuquerque failure to include security infraction notices in personnel security files.

Dec 1987

GAO/RCED-88-28/DOE Needs a More Accurate and Efficient Security Clearance Program. Inefficient security clearance program: clearance processing delays; inaccurate clearance data bases; need-to-know problems.

Apr 1988

DOE/IG-255/Timeliness in Processing DOE Headquarters Security Clearances. More than 100 days average time for processing applications after necessary forms initially completed; lack of accountability for tracking applications and ensuring timely processing; decisions based on investigative reports not made in timely manner.

Mar 1990

DOE/IG/WR-O-90-02/Nevada Operations Office Oversight of Management and Operating Contractor Security Clearances. Four areas employing 928 "Q" cleared employees who had no access to classified material and no clear need to know.

Apr 1990

DOE/IG-281/Inspection of LLNL's Drug-Free Workplace Program. Absence of random drug-testing program at Lawrence Livermore National Laboratory (LLNL), and no original plans to implement program without federal requirement.

Nov 1990

DOE/IG/WR-B-91-01/Richland Operations Office of Management and Operating Contractor Personnel Security Clearances. Insufficient number of trained staff in Personnel Security Branch; significant backlog of personnel security clearances awaiting adjudication.

Dec 1990

DOE/Safeguards and Security Task Force (Freeze Report). Security clearance processing time exceeds any reasonable standard; OPM delays in investigation not challenged by DOE; resources to implement Personnel Security Assurance Program not provided.

Sep 1991

DOE/IG/WR-B-91-08/Review of Contractor's Personnel Security Clearances at DOE Field Office, Albuquerque. Albuquerque Field Office granted "Q" clearances to 1,058 contractor lab and plant employees who did not need to access classified information.

Dec 1991

DOE/IG/WR-V-92-06/Audit of Internal Controls That Assure FY 1991 Costs Claimed by and Reimbursed to LANL Are Allowable Under DOE Contract #W-7405-ENG-36. LANL requested "Q" clearances for more than 500 people not needing access to classified information.

May 1992

DOE/IG-310/ General Management Inspection of the Department of Energy's Nevada Field Office. Defense personnel allowed access to SRD without full background investigation; security clearances

reinstated without conduct of required supplemental investigations; individuals designated "holders" for classified documents, without being assigned responsibility for safeguarding documents.

Mar 1993

DOE/IG-323/Review of DOE's Personnel Security Clearance Program. DOE granted security clearances to individuals not specifically requiring access to classified material; processing clear cases averaged 43 working days, 174 calendar days to process derogatory cases.

Aug 1993

DOE/IG/S9IJS010/Personnel Security Clearance Suspensions and Revocations at the DOE Albuquerque Field Office, Based Upon Security Infractions/Violations. Deficiencies and inconsistencies in handling of security infractions/incidents by certain national labs and processing of related personnel security actions by Albuquerque.

Aug 1993

GAO/RCED-93-183/Nuclear Security: DOE's Progress on Reducing Its Security Clearance Workload. Ineffective management by DOE of personnel security cases containing unfavorable information; some DOE contractors not verifying important information on prospective employees.

May 1995

DOE/IG/INS-L-95-07/Inspection of LANL-Alleged TA-55 Security Violation. LANL employees who were not personnel security assurance program cleared had been provided access to the material access area at TA-55 site.

Jun 1998

DOE/OCI/Mapping the Future of DOE's CI Program. Classified findings.

FOREIGN VISITORS AND ASSIGNMENTS

Dec 1986

DOE Special Project Team/Operation Cerberus Report. Scant data available at DOE headquarters on number and scope of foreign nationals at DOE facilities; approval authority for foreign visits and assignments not centralized.

Oct 1988

GAO/RCED-89-31/Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories. Failure to obtain timely and adequate information on foreign visitors before allowing them access to labs; lack of enforcement by DOE of internal control mechanisms for approving, monitoring, and reporting foreign visits; no internal review of foreign visitor program; no integrated system to obtain and disseminate foreign visitor information to DOE field offices; inattention to sensitive subjects discussed with foreigners.

Dec 1990

DOE Safeguards and Security Task Force/Freeze Report. Security would suffer little if records checks were to be discontinued.

Oct 1993

DOE/IG-337/Use of Intelligence Information to Identify the Foreign Interests of Entities Involved with DOE Programs. Failure by DOE to take action to implement provisions of Public Law 102-484 regarding award of certain departmental national security contracts to companies owned by entity controlled by foreign government.

Nov 1996

Deputy Secretary of Energy/Curtis Plan. Classified findings.

Sep 1997

GAO/RCED-97-229/DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories. Less than fully effective procedures for obtaining indices checks on foreign visitors and controlling dissemination of sensitive information. LANL allowed unescorted after-hours access to controlled areas, to preserve "open campus atmosphere." Lack of clear criteria for identifying visits that involve sensitive subjects. Result: sensitive subjects may have been discussed with foreign nationals without DOE knowledge and approval.

Dec 1997

DOE/IG/CR-L-989-02/FMFIA 1997. Large and increasing numbers of foreign nationals visiting labs raised concern about access and potential compromises of classified, sensitive, and proprietary information.

Oct 1998

GAO/T-RCED-99-19/Department of Energy: Problems in DOE's Foreign Visitors Program Persist. As in 1988, visitors with ties to foreign intelligence services gained access to laboratories without DOE and/or laboratory officials' advance knowledge of visitors' connections. As found by GAO in 1988 and 1997, procedures for identifying sensitive subjects lack clear criteria and controls to ensure that visits potentially involving such subjects are reviewed by DOE.

Jun 1998

DOE/OCI/Mapping the Future of DOE's CI Program. Classified findings.

Feb 1999

DOE/IG/CR-L-99-01/FMFIA 1998. Large and increasing numbers of foreign nationals visiting labs raised concern about access and potential compromises of classified, sensitive, and proprietary information.

INFORMATION SECURITY.

Sep 1982

DOE/OSS Inspection Report on Albuquerque Area Office, LANL, SNL, and Rocky Flats Plant Classified finding.

May 1984

DOE/OSQ Assessment: LANL, SNL, LLNL. Classified findings.

Jan 1985

DOE/OSQ Assessment: Inspection Report on Albuquerque Area Office, LANL, Mound Facility. Classified findings.

Feb 1985

DOE/OSQ Assessment: Inspection Report on DOE Germantown and Forrestal locations. Classified findings.

Mar 1985

DOE/OSQ Assessment: Albuquerque Operations Office, SNL. Classified findings.

Jun 1985

DOE/OSQ Assessment: Inspection Report on SNL and SNLL and San Francisco Operations Office. Classified findings.

Nov 1986

DOE/OSQ Assessment: Inspection Report on LANL, Albuquerque Area Office. Classified findings.

Jan 1987

DOE/OSE: Inspection Report on DOE Headquarters. Classified findings.

Apr 1987

DOE/OSE: Inspection Report on San Francisco Operations Office and SNLL. Classified findings.

Jun 1987

DOE/OSE: Inspection Report on Albuquerque Operations Office, SNL, and LANL. Classified findings.

Apr 1990

DOE/Annual Report to the President on the Status of Domestic Safeguards and Security at All Nuclear Weapons Facilities. Classified findings.

Dec 1990

Safeguards and Security Task Force/Freeze Report. Inadequate oversight and control over Secret

document inventory; responsibility for classified and unclassified computer security split between two DOE organizations, thereby diluting computer security expertise; inadequate professional development programs for computer security specialists.

Feb 1991

GAO/RCED-91-65/Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate. Inadequate accountability for documents at Lawrence Livermore National Laboratory (LLNL) classified; 1990 GAO inventory identified 12,000 missing secret documents. As of January 1991, over 10,000 still missing.

1986; Jul 1991

GAO/RCED-91-183/DOE Original Classification Authority Has Been Improperly Delegated. Untitled Information Security Oversight Office report. Improper delegation of original classification authority to contractors, in violation of E.O. 12356, 1982.

Jul 1991

DOE/Annual Report to the President on the Status of Safeguards and Security at All Domestic Nuclear Weapons Facilities. Classified findings.

Nov 1992

DOE/OSE Annual Report: Safeguards and Security Oversight During Fiscal Year 1992. Lack of adequate guidance; fragmented approach for protecting information.

Feb 1993

DOE/OSS/1992 Annual Report to Secretary. Less than satisfactory ratings in classified matter protection and control.

Jan 1994

DOE/OSS/Status of Safeguards and Security, Fiscal Year 1993. Inability of DOE to identify its most sensitive information; failure to properly accredit systems processing classified information; lack of controls to provide access authorities and proper password management; no configuration management; improper labeling of magnetic media; failure to perform management reviews.

Apr 1994

DOE/Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. At LLNL, decentralized computer security management lacked aggressive technical oversight and complete enforcement of critical program elements; computer security program application favors users at expense of security implementation. (U)

Jun 1995

DOE/Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. Improper accreditation of laptops; data transferred from higher classified systems to lower systems without proper review; inadequate audit trails; improper password

controls.

Jan 1996

DOE/OSS/Status of Safeguards and Security, Fiscal Year 1995. Lack of management attention to basic information assurance concerns at a time of "increased interconnectivity with relatively uncontrolled entities."

Jan 1997

DOE/OSS/Status of.Safeguards and Security, Fiscal Year 1996. Computer system interconnectivity growing exponentially, increasing risk to DOE information assets.

Jun 1998

DOE/OCI/Mapping the Future of DOE's CI Program. Classified findings.

1998

DOE/IG/198AL001 Improper Export of Software. LANL improperly transferred particular computer software program to PRC and Russia; no criminal violations found, but LANL failed to obtain proper US Department of Commerce license approval.

Nov 1998

DOE/OSE/Safeguards and Security Inspection of LANL. Classified findings.

Apr 1999

GAO/Key Factors Underlying Security Problems at DOE Facilities (April 20, 1999 GAO Congressional testimony). Inadequate separation of classified and unclassified computer networks at LANL in 1988, 1992, and 1994; classified information discovered on LANL unclassified computer network in 1998.

1999

DOE/23rd Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities. Numerous incidents of classified information being placed on unclassified systems, including several since the development of a corrective action plan in July 1998.

SECURITY MANAGEMENT, PLANNING, AND OVERSIGHT.

Jun 1985

DOE/OSQ Assessment: Inspection Report on SNLL, LLNL, San Francisco Operations Office. Classified findings.

Jan 1986

U.S. House of Representatives: Letter of Rep. Dingell to the President. Misleading system of rating

DOE inspections of safeguards and security.

Dec 1986

DOE/Special Project Team/Cerberus Report. Lack of adequate short- and long-term planning in DOE's safeguards and security program; insufficient intelligence support for DOE facility security; insufficient standardization of security methods, equipment, and strategies at DOE weapons sites.

Jun 1988

DOE Annual Report to the President on Domestic Safeguards and Security. Classified findings.

Oct 1990
Mar 1991

GAO/RCED-91-12/Potential Security Weaknesses at Los Alamos and Other DOE Facilities and *GAO/RCED-92-39/Nuclear Security: Safeguards and Security Weaknesses at DOE's'Weapons Facilities.* Inability of DOE to track, monitor, and correct security deficiencies at DOE facilities.

Dec 1990

Safeguards and Security Task Force/Freeze Report. Classified findings.

Feb 1991

GAO/RCED-91-65/ Nuclear Security: Accountability for Livermore's Secret Classified Documents is Inadequate. Inadequate DOE oversight of LLNL's document control program.

Mar 1991

GAO/RCED-91-83/DOE Needs Better Controls to Identify Contractors Having Foreign Interests. Inadequate controls for identifying DOE contractors having foreign interests.

Jun 1992

GAO/RCED-92-146/Weak Internal Controls Hamper Oversight of DOE's Security Program. Lack of system at DOE to oversee and monitor exceptions to DOE safeguards and security orders.

Oct 1992

GAO/RCED-93-14/Safeguards and Security Planning at DOE Facilities Incomplete. Incomplete safeguards and security planning at DOE facilities. As of fall 1992, DOE had not completed plans for 15 of its 27 sensitive facilities.

Nov 1992

DOE/OSE/Annual Report: Safeguards and Security Oversight During Fiscal Year 1992. Numerous overlapping and confusing safeguards and security inspections; management and oversight problems represent most significant weaknesses in DOE's security program; inadequate life cycle planning of security systems.

Nov 1992

GAO/RCED-93- 10/Improving Correction of Security Deficiencies at DOE's Weapons Facilities. Insufficient DOE validation of corrective actions.

Feb 1993

DOE/Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security. In Violation of Laws, Losses, and Incidents of Security Concern Program, lack of management focus resulted in personnel seldom being held responsible for disregard of security requirements.

Jan 1994

DOE/OSS/Status of Safeguards and Security, Fiscal Year 1993. No single office at DOE Headquarters responsible for safeguards and security program; duplication of guidance, unnecessary requests for information, inefficient program execution.

Nov 1996

Deputy Secretary of Energy/Curtis Plan. Classified findings.

Sep 1997

GAO/RCED-97-229/Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories. Failure to provide detailed oversight of the national laboratories' CI programs.

1997

DOE/OSA/Report to Secretary on Status of DOE Safeguards and Security Program. Fragmented and dysfunctional security management structure.

Oct 1998

GAO/T-RCED-99-19/Department of Energy: Problems in DOE's Foreign Visitor Program Persist. Failure to evaluate effectiveness of security controls over information in laboratory areas most frequented by foreign visitors.

1998

DOD/NCCS Support Staff/DOE Nuclear Weapons-Related Security Oversight Process. Classified findings.

Jan 1999

Special Security Review/Internal Report to the Secretary. Classified findings.

COUNTERINTELLIGENCE.

Jun 1990

Classified report.

Apr 1992

Classified report.

Apr 1997

GAO/RCED-97-128R/Department of Energy: Information on the Distribution of Funds for Counterintelligence Programs and the Resulting Expansion of These Programs. Indirect and inconsistent funding for CI programs; despite additions to overall CI program funds, eight DOE facilities significantly reduced budgetary support for their CI programs.

Apr 1997

Classified report.

Sep 1997

GAO/RCED-97-229/Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories. DOE CI programs not based on comprehensive assessment of foreign espionage threat.

Jun 1998

DOE/OCI/Mapping the Future of DOE's CI Program. Classified findings.

On to Next Section

Back to Report Top Page

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the
U.S. Department of Energy

INTELLIGENCE COMMUNITY DAMAGE ASSESSMENT OF CHINA'S ACQUISITION OF U.S. NUCLEAR WEAPONS INFORMATION

Chinese strategic nuclear efforts have focused on developing and deploying a survivable long-range missile force that can hold a significant portion of the U.S. and Russian populations at risk in a retaliatory strike. By at least the late 1970s the Chinese launched an ambitious collection program focused on the U.S., including its national laboratories, to acquire nuclear weapons technologies. By the 1980s China recognized that its second strike capability might be in jeopardy unless its force became more survivable. This probably prompted the Chinese to heighten their interest in smaller and lighter nuclear weapon systems to permit a mobile force.

China obtained by espionage classified U.S. nuclear weapons information that probably accelerated its program to develop future nuclear weapons. This collection program allowed China to focus successfully down critical paths and avoid less promising approaches to nuclear weapons designs.

- China obtained at least basic design information on several modern U.S. nuclear reentry vehicles, including the Trident II (W-88).
- China also obtained information on a variety of U.S. weapon design concepts and weaponization features, including those of a neutron bomb.
- We cannot determine the full extent of weapon information obtained. For example, we do not know whether any weapon design documentation or blueprints were acquired.
- We believe it is more likely that the Chinese used U.S. design information to inform their own program than to replicate U.S. weapon designs.

China's technical advances have been made on the basis of classified and unclassified information derived from espionage, contact with U.S. and other countries' scientists, conferences and publications, unauthorized media enclosures, declassified U.S. weapons information, and Chinese indigenous development. The relative contribution of each cannot be determined.

Regardless of the source of the weapons information, it has made an important contribution to the Chinese objective to maintain a second strike capability and provided useful information for future designs.

Significant deficiencies remain in the Chinese weapons program. The Chinese almost certainly are using aggressive collection efforts to address deficiencies as well as to obtain manufacturing and production capabilities from both nuclear and nonnuclear sources.

To date, the aggressive Chinese collection effort has not resulted in any apparent modernization of their deployed strategic force or any new nuclear weapons deployment.

China has had the technical capability to develop a multiple independently targetable reentry vehicle (MIRV) system for its large, currently deployed ICBM for many years, but has not done so. U.S. information acquired by the Chinese could help them develop a MIRV for a future mobile missile.

We do not know if U.S. classified nuclear information acquired by the Chinese has been passed to other countries. Having obtained more modern U.S. nuclear technology, the Chinese might be less concerned about haring their older technology.

On to Next Section

Back to Report Top Page

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

PRESIDENTIAL DECISION DIRECTIVE NO. 61

The Department of Energy (DOE) has stewardship of vital national security capabilities, from nuclear weapons to leading edge research and development projects. These capabilities, and related DOE programs, are important not only to the strength of our Nation, but within the framework of international cooperation, to the lessening of global threats. We must therefore ensure the security of these critical programs through the application of an effective and coordinated counterintelligence (CI) program. To enhance counterintelligence capabilities at DOE, President Clinton directed in February 1998 that the following initiatives be implemented:

The CI and foreign intelligence (FI) elements of DOE will be reconfigured into two independent offices, which will report directly to the Secretary of Energy. The Secretary may delegate regular management of these two offices to the Deputy Secretary.

The Director of the new Office of CI (OCI) will be a senior executive from the Federal Bureau of Investigation (FBI). The OCI will be staffed by DOE CI professionals, augmented by detailees from other Intelligence Community agencies as appropriate.

The Director, OCL will have direct access to the Secretary of Energy, the Director of Central Intelligence (DCI), and the Director, FBI.

All CI and FI activities at DOE and the laboratories will continue to be included in the National Foreign Intelligence Program and, as such, are subject to policy and programmatic guidance by the DCI and applicable Congressional oversight.

The laboratory directors will be directly accountable to the Secretary of Energy for the performance of the CI program at their locations. Existing DOE contracts with the labs will be amended to include CI program goals and objectives and performance measures to evaluate compliance with those contractual obligations. CI personnel assigned to the laboratories will have direct access to the laboratory directors and will concurrently report to the Director, OCI. CI oversight functions previously designated to DOE operations and field offices will revert to the OCI.

The National CI Policy Board (NACIPB) will oversee implementation of the Directive and will continue to coordinate and/or provide other CI community resources, support and oversight to the DOE CI program as needed.

When appropriate, the NACIPB may refer problems and concerns not resolved by the NACIPB and Director, OCI, to the Energy Security Management Board, established by the National Defense Authorization Act for Fiscal Year 1998.

The incoming Director, OCI, will prepare a report for the Secretary of Energy ninety days after his arrival, to include progress on the initiative, a strategic plan for achieving long–term goals, and recommendations on whether and to what extent other organizational changes may be necessary to strengthen CI. In preparing the report, the Director will consult with laboratory directors and other appropriate DOE personnel.

The Director, OCI, will initiate an internal inspection process to review annually DOE's CI program and provide results to the Secretary of Energy.

The Secretary of Defense, Attorney General, DCI, and Director, FBI, as involved principals, will provide support to the Secretary of Energy in the implementation of the directive and continuation of an effective CI program. Such support will include provision of personnel, investigative and analytic resources. These principals will receive copies of the initial ninety–day report of the Director, OCI, the annual inspection reports of the CI program and any reports generated by the Director, OCI, concerning significant policy or operational issues.

The new CI and FI offices will ensure that their operational and analytic efforts and results are integrated, mutually and throughout DOE and the laboratories, to provide the greatest level of protection to our national security interests. The OCI and DOE Office of Security Affairs will, in coordination, develop and implement specific security measures to reduce the threat to classified and sensitive information at DOE, its field activities and the national laboratories. The Office of Security Affairs will provide timely notification to the OCI of any potential CI problems developed through these procedures.

The Secretary of Energy will establish an Office of Foreign Visits and Assignments at DOE Headquarters to facilitate the participation of qualified foreign nationals in DOE projects. The Secretary will develop procedures and practices for this Office which will meet the needs of DOE's vital national security programs while providing protection from possible foreign threats.

Within 120 days, the Secretary of Energy will advise the Assistant to the President for National Security Affairs on the actions taken and specific remedies designed to implement this directive.

On to Next Section

Back to Report Top Page

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy

BIBLIOGRAPHY OF MAJOR UNCLASSIFIED SOURCES

Note: The following list does not include citations for several hundred classified reports and documents provided to the PFIAB by CIA, FBI, DOE, NSA, DOD, and DOJ.

Boyer, Paul, *By the Bomb's Early Light: American Thought and Culture at the Dawn of the Atomic Age.* Chapel Hill: University of North Carolina Press, 1985.

Department of State memorandum, "China Arms Control Exchange Workshops," undated

DOE chronology, April 13, 1999

DOE Field Fact Book, May 1998

DOE, "Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," June 1995

DOE, "Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," September 1996

DOE, "Department of Energy First Tier Organizations, Terms of Office," undated

DOE, Office of Counterintelligence, "The Foreign Intelligence Threat to Department of Energy Personnel, Facilities and Research, Summary Report," August 1990

DOE, "Office of Safeguards and Security Inspection Report on Albuquerque Area Office, Los Alamos National Laboratory, Sandia National Laboratory, and Rocky Flats Plant," September 1982

DOE, "Office of Safeguards and Security, Report to the Secretary: Status of Safeguards and Security," February 1993

DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1993," January 1994

DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1994," January 1995

DOE, "Office of Safeguards and Security, Status of Safeguards and Security, Fiscal Year 1995," January 1996

DOE, "Office of Security Affairs: Report to the Secretary on the Status of the DOE Safeguards and Security Program," November 1997

DOE, "Office of Security Evaluations Annual Report: Safeguards and Security Oversight During Fiscal Year 1992," November 1992

DOE, "Office of Security Evaluations: Inspection Report on DOE Headquarters," January 1987

DOE, Office of Security Affairs, "Report on the Status of the Department of Energy's Safeguards and Security Program, October 1997," November 6, 1997

DOE, "Plutonium: The First 50 Years. United States Plutonium Production, Acquisition, and Utilization from 1944 Through 1994

DOE, Robert Daniel memorandum to Secretary Watkins, January 12, 1993

DOE, Special Project Team, "Operation Cerberus Report," December 1986

DOE/IG/198AL001, "Improper Export of Software," 1998

DOE/IG/CR-L-989-02, "FMFIA 1997," December 1997

DOE/IG/CR-L-99-01, "FMFIA 1998," February 1999

DOE/IG/INS-L-92-02, "Control of Classified Documents at DOE Savannah River Operations Office," May 1992

DOE/IG/INS-L-95-07, "Inspection of Los Alamos National Laboratory: Alleged TA-55 Security Violation," May 1995

DOE/IG/INS-O-94-05, "Inspection of Physical Security Operations at Los Alamos TA-18 Site," August 1994

DOE/IG/S941S012, "Albuquerque Vault Classification," March 1995

DOE/IG/S9IJS010, "Personnel Security Clearance Suspensions and Revocations at the DOE Albuquerque Field Office, Based Upon Security Infractions/Violations," August 1993

DOE/IG/WR-B-91-01, "Richland Operations Office of Management and Operating Contractor Personnel Security Clearances," November 1991

DOE/IG/WR-B-91-08, "Review of Contractor's Personnel Security Clearances at DOE Field Office, Albuquerque," September 1991

DOE/IG/WR-O-90-02, "Nevada Operations Office Oversight of Management and Operating Contractor Security Clearances," March 1990

DOE/IG/WR-V92-06, "Audit of Internal Controls That Assure FY 1991 Costs Claimed by and Reimbursed to Los Alamos National Laboratory Are Allowable Under DOE Contract #W-7405-ENG-36," December 1991

DOE/IG-228, "Retention of Security Clearances at DOE Headquarters," July 1986

DOE/IG-238, "Selected Aspects of DOE's Personnel Security Program," May 1987

DOE/IG-255, "Timeliness in Processing DOE Headquarters Security Clearances," April 1988

DOE/IG-281, "Inspection of Lawrence Livermore National Laboratory's Drug-Free Workplace Program," April 1990

DOE/IG-296, "Department-Wide Audit of the Visibility Over the Status of Nuclear Materials," August 1991

DOE/IG-310, "General Management Inspection of the Department of Energy's Nevada Field Office," May 1992

DOE/IG-319, "Administration of Conflict of Interest Relating to Technology Transfer at Los Alamos National Laboratory," January 1993

DOE/IG-323, "Review of DOE's Personnel Security Program," March 1993

DOE/IG-385, "Special Audit Report on the Department of Energy's Arms and Military-Type Equipment," February 1, 1996

DOE, "Response to the Cox Commission Report: The Benefits of Department of Energy International Scientific and Technical Exchange Programs," April 1999

GAO/Key Factors Underlying Security Problems at DOE Facilities," (Statement of Victor S. Rezendes, Director, Energy, Resources and Science Issues, Resources, Community, and Economic Development Division, GAO, in testimony before the Subcommittee on Oversight and Investigations, Committee on Commerce, House of Representatives), April 20, 1999

GAO/AIMD-95-165, "Department of Energy: Poor Management of Nuclear Materials Tracking Capabilities Are Limited," August 3, 1995

GAO/EMD-79-109, "DOE's Erroneous Declassification of Nuclear Weapons Design Document," September 21, 1979

GAO/EMD-80-38, "Nuclear Fuel Reprocessing and the Problems of Safeguarding Against the Spread of Nuclear Weapons," March 18,1980

GAO/RCED-86-144, "Nuclear Nonproliferation: DOE Has Insufficient Control Over Nuclear Technology Exports," May 1, 1986

GAO/RCED-87-150, "Nuclear Nonproliferation: Department of Energy Needs Tighter Controls Over Reprocessing Information," August 17, 1987

GAO/RCED-87-72, "Nuclear Security: DOE's Reinvestigation of Employees Has Not Been Timely,"

March 10, 1987

GAO/RCED-88-28, "Nuclear Security: DOE Needs a More Accurate and Efficient Security Clearance Program," December 29, 1987

GAO/RCED-89-116, "Nuclear Nonproliferation: Better Controls Needed Over Weapons-Related Information and Technology," June 19, 1989

GAO/RCED-89-31, "Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories," October 11, 1988

GAO/RCED-89-34, "Nuclear Security: DOE Actions to Improve the Personnel Clearance Program," November 9, 1988

GAO/RCED-90-122, "Nuclear Security: DOE Oversight of Livermore's Property Management System is Inadequate," April 18, 1990

GAO/RCED-91-12, "Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities," October 1990

GAO/RCED-91-183, "Nuclear Security: DOE Original Classification Authority Has Been Improperly Delegated," July 5, 1991

GAO/RCED-91-65, "Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate," February 8, 1991

GAO/RCED-91-83, "Nuclear Nonproliferation: DOE Needs Better Controls to Identify Contractors Having Foreign Interests," March 25, 1991

GAO/RCED-91-141, "Nuclear Security: Property Control Problems at DOE's Livermore Laboratory Continue," May 16, 1991.

GAO/RCED-92-146, "Nuclear Security: Weak Internal Controls Hamper Oversight of DOE's Security Program," June 29, 1992

GAO/RCED-92-39, "Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities," December 13, 1991

GAO/RCED-93-10, "Nuclear Security: Improving Correction of Security deficiencies at DOE's Weapons Facilities," November 16, 1992

GAO/RCED-93-14, "Nuclear Security: Safeguards and Security Planning at DOE Facilities Incomplete," October 30, 1992

GAO/RCED-93-183, "Nuclear Security: DOE's Progress on Reducing Its Security Clearance Work Load," August 12, 1993

GAO/RCED-93-23, "Personnel Security: Efforts by DOD and DOE to Eliminate Duplicative Background Investigations," May 10, 1993

GAO/RCED/AIMD-95-5, "Nuclear Nonproliferation: U.S. International Nuclear Materials Tracking

Capabilities are Limited," December 27, 1994

GAO/T-RCED-96-260, DOE Security: Information on Foreign Visitors to the Weapons Laboratories, undated

GAO/RCED-97-128R, "Department of Energy: Information on the Distribution of Funds for Counterintelligence Programs and the Resulting Expansion of These Programs," April 25, 1997

GAO/RCED-97-229, "Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories," September 25, 1997

GAO/RCED-99-19, "Department of Energy: Problems in DOE's Foreign Visitor Program Persist, October 6, 1998

GAO/RCED-99-54, "Nuclear Nonproliferation: Concerns With DOE's Efforts to Reduce the Risks Posed by Russia's Unemployed Weapons Scientists," February 19, 1999

Hewlett, Richard G. and Francis Duncan, *Atomic Shield: A History of the United States Atomic Energy Commission*. May 1969

Los Alamos National Laboratory, "Draft Chronology," undated

New York Times, "Abstract," August 5, 1977

Representative John Dingell letter to the President of the United States, January 28, 1986

Representative John Dingell letter to Warren Rudman, March 24, 1999

Senate Armed Services Committee, Transcript of Committee Hearing, April 12, 1999

US Congress, "DOE, and Congressional Committee Jurisdiction," June 3, 1999

US Nuclear Command and Control System Support Staff, "Assessment Report: Department of Energy Nuclear Weapons-Related Security Oversight Process," March 1998 (FOUO)

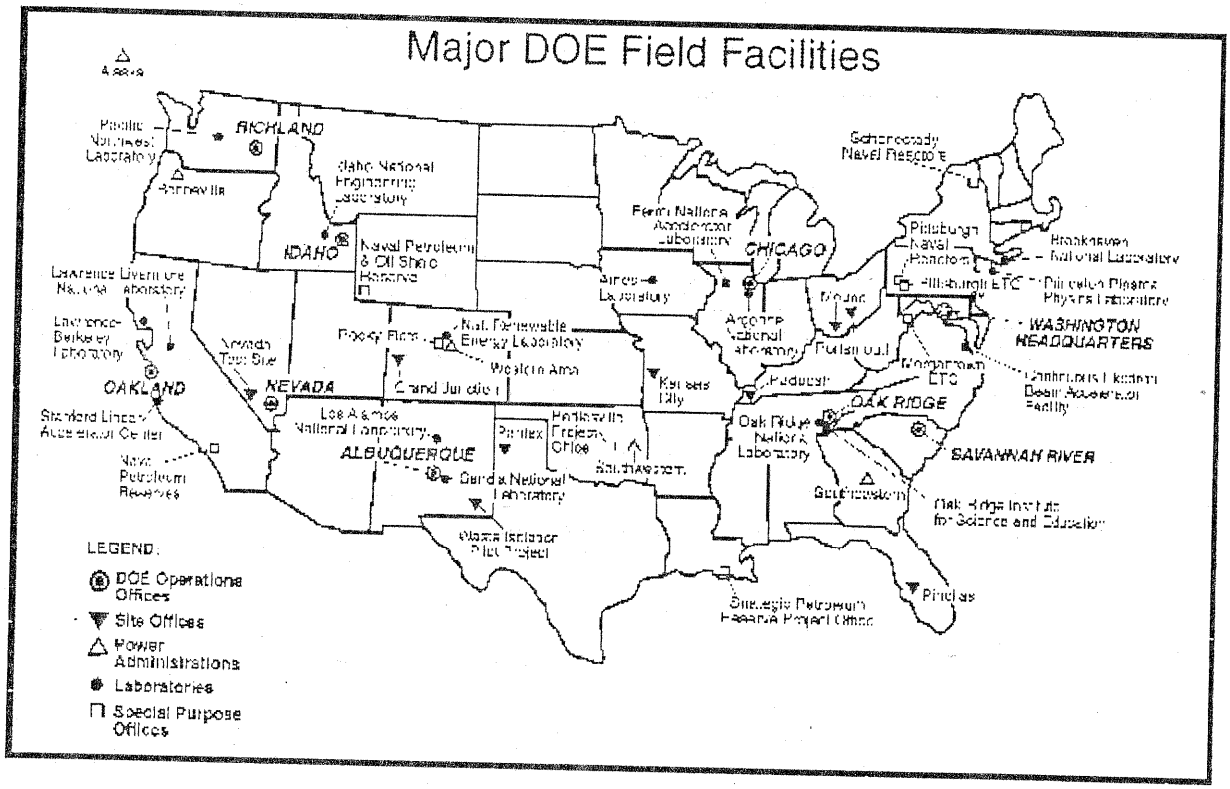
On to Map of DOE Facilities

Back to Report Top Page

FAS | Secrecy | PFIAB Top Page ||| Index | Search | Join FAS

SCIENCE AT ITS BEST
SECURITY AT ITS WORST

A Report on Security Problems at the U.S. Department of Energy



SOURCE: U.S. DEPT. OF ENERGY

Back to Report Top Page

5

Department of Energy
Washington, D.C.

ORDER
DOE O 470.1

Approved: 9-28-95
Sunset Review: 9-29-97
Expires: 9-29-99
Change 1: 6-21-96

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. OBJECTIVES.

a. To ensure appropriate levels of protection against unauthorized access; theft, diversion, loss of custody, or destruction of nuclear weapons, or weapons components; espionage; loss or theft of classified matter or Government property; and other hostile acts that may cause unacceptable adverse impacts on national security or on the health and safety of Department of Energy (DOE) and contractor employees, the public, or the environment.

b. To deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of special nuclear materials.

c. To provide an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information, nuclear materials, nuclear weapons, nuclear weapons components, and DOE and certain DOE contractor property and personnel as required by the Atomic Energy Act of 1954, as amended, other Federal statutes, Executive orders, and other directives.

d. To use the Design Basis Threat Policy, issued by the Director of Security Affairs, in the design and implementation of protection programs.

e. To provide levels of protection in a graded manner in accordance with the potential risks.

f. To establish safeguards and security programs comparable in effectiveness to other Federally regulated programs with similar interests when such levels are consistent with DOE protective needs and national security interests.

g. To ensure effective planning of graded protection levels and prudent application of resources.

h. To ensure personnel receive training appropriate for their roles in support of the program and

that persons given access authorization are aware of Safeguards and Security Program requirements.

i. To standardize safeguards and security equipment and systems to achieve operational and financial benefits.

2. CANCELLATIONS. The Orders listed below are canceled. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with such an Order. Canceled Orders which are incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Orders.

a. DOE 5630.11B, SAFEGUARDS AND SECURITY PROGRAM, of 8-2-94.

b. DOE 5630.13A, MASTER SAFEGUARDS AND SECURITY AGREEMENTS, of 6-8-92.

c. DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING, of 6-9-92.

d. DOE 5630.15, SAFEGUARDS AND SECURITY TRAINING PROGRAM, of 8-21-92.

e. DOE 5630.16A, SAFEGUARDS AND SECURITY ACCEPTANCE AND VALIDATION TESTING PROGRAM, of 6-3-93.

f. DOE 5630.17, SAFEGUARDS AND SECURITY (S&S) STANDARDIZATION PROGRAM, of 9-29-92.

g. DOE 5631.1C, SAFEGUARDS AND SECURITY AWARENESS PROGRAM, of 5-4-94.

h. DOE 5631.4A, CONTROL OF CLASSIFIED VISITS, of 7-8-92.

i. DOE 5634.1B, FACILITY APPROVALS, SECURITY SURVEYS, AND NUCLEAR MATERIALS SURVEYS, of 9-15-92.

j. DOE 5634.3, FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM, of 6-14-93.

k. DOE 5639.3, VIOLATION OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 9-15-92.

l. Chapter XI, "Protection Element: Acceptance and Validation Testing," in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94.

3. APPLICABILITY.

a. DOE Elements. DOE Elements responsible for safeguards and security activity and/or the protection and control of safeguards and security interests.

b. Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (Attachment 1) sets forth requirements that are to be applied to the covered contractors.

c. Exclusions. DOE facilities and activities regulated by the Nuclear Regulatory Commission.

4. REQUIREMENTS. General Safeguards and Security Program requirements are listed below and in the chapters appended to this Order. Detailed requirements for personnel security activities, protection operations, information security, and materials control and accountability are set forth

the Orders listed in subparagraph a below. Note that terms commonly used in the Safeguards and Security Program are defined in the "Safeguards and Security Definitions Guide," which is maintained by the Office of Safeguards and Security.

a. Key Safeguards and Security Program Elements.

(1) Program Management, DOE O 470 series.

(2) Personnel Security, DOE O 472 series.

(3) Protection Operations, DOE 5632 and DOE O 473 series.

(4) Materials Control and Accountability, DOE 5633 and DOE O 474 series.

(5) Information Security, DOE 5639 and DOE O 471 series.

b. Risk Management. The determination of the appropriate level of protection against risk shall consider the nature of the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act. Accordingly, safeguards and security programs shall be based on vulnerability/risk analyses designed to provide graded protection in accordance with the asset's importance or the impact of its loss, destruction, or misuse. Risks to be accepted by the Department shall be identified and documented by vulnerability/risk analyses.

c. Graded Protection. By graded approach, DOE intends that the highest level of protection be given to security interests whose loss, theft, compromise, and/or unauthorized use will seriously affect the national security, and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs. Protection of other interests shall be graded accordingly. Asset valuation, threat analysis, and vulnerability assessments shall be considered, along with the acceptable level of risk and any uncertainties, to decide how great is the risk and what protection measures are to be applied.

It should be recognized that risks will be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

d. Site-Specific Programs. Safeguards and security programs shall be tailored to address site-specific characteristics. e. Planning. Chapter I sets forth detailed requirements for site-wi maintained at the Operations Office, or equivalent-level, and for other plans to address specific needs.

f. Deviations. Alternate or equivalent means of providing adequate safeguards and security may be proposed to meet a specific requirement of this and other Safeguards and Security Program directives. In some cases, it may be justifiable not to meet a requirement by any means. The following procedures and approval levels shall apply to all such deviations from Safeguards and Security Program directives' requirements. Any extensions to the approved period of time for deviations shall require reapplication for approval.

(1) Variances are approved conditions that technically vary from a Safeguards and Security directive's requirement, but afford equivalent levels of protection without compensatory measures.

(a) Variances shall be approved by the Head of a Field Element. The Office of Safeguards and Security and appropriate program offices shall be notified.

(b) For Headquarters Elements, the cognizant Secretarial Officer shall approve

variances with the concurrence of the Director, Headquarters Operations Division, Office of Safeguards and Security.

(c) Variances may be approved for an indefinite period.

(2) Waivers are approved nonstandard conditions that deviate from a Safeguards and Security directive's requirement which, if uncompensated, would create a potential or real safeguards and security vulnerability. Waivers therefore require implementation of compensatory measures for the period of the waiver (e.g., expenditure of additional resources to implement enhanced protection measures).

(a) Waivers shall be approved by Heads of Field Elements provided:

1 the cognizant Secretarial Officer(s) and the Office of Safeguards and Security are notified 30 days in advance of such approval;

2 comments provided by Headquarters Elements are considered before approving the waiver;

3 adequate compensatory measures are in place; and

4 performance testing is accomplished, if appropriate.

(b) Waivers for Headquarters Elements may be approved by the cognizant Secretarial Officer providing:

1 the Office of Safeguards and Security is notified 30 days in advance of approval and the Director, Headquarters Operations Division has concurred in the waiver; and

2 the requirements of subparagraphs 4f(2)(a)3 and 4 above are met.

(c) A waiver shall not exceed 2 years. Extensions may be requested using the same process.

(3) Exceptions are approved deviations from a Safeguards and Security directive's requirement that create a safeguards and security vulnerability. Exceptions shall be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk. An exception must be approved by both the Secretarial Officer and the Director of Security Affairs.

(a) For Field Elements, exception requests shall be submitted through line management to the cognizant Secretarial Officer and to the Director of Security Affairs for review and approval.

(b) For Headquarters Elements, exception requests shall be submitted through the Headquarters Operations Division for review and approval by the cognizant Secretarial Officer and the Director of Security Affairs.

(c) Exceptions shall not exceed 3 years. Extensions may be requested using the same process.

(d) The need for an exception shall be validated annually.

(e) Exceptions shall be included in Site Profiles, which form the basis for the DOE's Annual Report to the President on the Status of Safeguards and Security.

(4) Documentation. Specific information to be included to document each deviation is

provided in Appendix 1. Approved deviations shall be documented in safeguards and security documents. A deviation request approved out of cycle with the safeguards and security plan formulation and approval process shall be documented as an attachment to the applicable safeguards and security plan.

(5) Vulnerability Assessments and Performance Testing. Compensatory measures implemented and used as the basis for an exception request shall be subject to formal vulnerability assessments and must be tested and validated by the cognizant Field Element. The results of the vulnerability assessment(s) and tests shall be doc security plan. Performance testing and documentation, as necessary, may also be required for waivers.

(6) Visits. Office of Safeguards and Security and affected program office representatives may perform on-site reviews, assessments, and validation visits to ascertain the nature and impact of deviation requests.

(7) Corrective Actions. Heads of DOE Elements shall monitor corrective actions, establish schedules, ensure that funding is effectively managed to address safeguards and security interests, and monitor compliance with schedules.

g. Standardization.

(1) Safeguards and security equipment and systems shall be selected on the basis of providing a benefit to DOE such as worker safety, compliance with life safety codes, enhancing mission capability, cost advantages, or facilitating contingency efforts.

(2) New facility designs shall incorporate the use of standardized safeguards and security equipment and systems where possible without compromising design flexibility or adherence to performance criteria.

h. Management Review of Safeguards and Security Programs. Individuals assuming Head of Field Element positions shall complete a status review for their safeguards and security programs. Within 15 calendar days of the review, a written report that identifies any significant deficiencies and corrective actions being taken or planned shall be sent to the Under Secretary or cognizant Program Office, as appropriate, with a copy to the Director of Security Affairs.

5. RESPONSIBILITIES.

a. Secretarial Officers.

(1) Provide program and project direction consistent with the Safeguards and Security directives and policy requirements.

(a) In coordination with the Director of Nonproliferation and National Security.

1 Ensure adequate protection is afforded safeguards and security interests.

2 Establish action criteria, including curtailment or suspension of operations, for operations that would result in an immediate and **unacceptable risk** to national security, the health and safety of employees, the public, or the environment. (b) Coordinate construction or alteration projects security interest with the Director of Security Affairs and the Associate Deputy Secretary for Field Management.

(c) Request establishment of safeguards and security activities and facility clearance(s) through the Office of Safeguards and Security. Notify the Office of

Safeguards and Security to terminate registration of such activities and facility clearances.

(2) Implement a security program consistent with the Headquarters Security Plan for Washington, D.C. area facilities and programs.

(3) Approve or disapprove requests for exceptions from Safeguards and Security directives' requirements in accordance with paragraph 4f(3)(a) to (e).

(4) Ensure that each request for a procurement requiring application of this Order incorporates the requirements specified in the Contractor Requirements Document (Attachment 1).

(a) Designate individual(s) to notify contracting officers of each procurement falling within the scope of this Order. Unless another individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization").

(b) Ensure the following:

1 The contracting officer provides DOE F 5634.2, "Contract Security Classification Specification," to the servicing safeguards and security office.

2 The contract clauses set forth in the DOE Federal Acquisition Regulation and other relevant sections of 48 CFR Chapter IX are included in contracts, as applicable.

3 The contracting officers incorporate provisions implementing the requirements of this Order in new and existing contracts that involve access authorizations, classified information, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or Departmental property valued at more than $5,000,000.

4 Contractual coverage is in place to permit implementation of this Order with regard to the contractor's nuclear materials activities before (as defined in 10 CFR Part 50) contractor.

5 Non-DOE funded work under their jurisdiction is provided protection in accordance with the Departmental safeguards, security, and classification policies.

(c) Appoint within their contracting activity a trained DOE employee as the Foreign Ownership, Control, and Influence (FOCI) point-of-contact.

(5) Ensure that safeguards and security budget proposals are adequate, and that resources are provided to implement them.

(6) Participate in the development and review of policy and standards for safeguards and security interests.

(7) Identify technological needs to the Office of Security Affairs for consideration in the safeguards and security technology development program.

(8) Implement the Classified Visits Program in accordance with Chapter VIII.

(a) Designate specific facilities where visits may be made only with the approval of the organization having program responsibility, and inform Heads of DOE Elements.

(b) Maintain records of individuals approved by their organizations to have continuing access on the basis of DOE Q and L access authorizations or Department of Defense or National Aeronautics and Space Administration certifications, and notify the Director of Safeguards and Security when such approvals are granted or canceled.

(9) Approve Site Safeguards and Security Plans and annual revisions thereto.

b. The Director of Nonproliferation and National Security shall, in addition to the duties shown in paragraph 5a, direct and coordinate the policy and procedures for a comprehensive Safeguards and Security Program.

(1) Through the Director of Security Affairs.

(a) Establish safeguards and security policies, requirements, standards, and guidance for DOE operations, including design basis threat, for use in designing and implementing DOE protection programs.

(b) Provide advice and assistance concerning safeguards and security programs, and coordinate with appropriate DOE organizations to correct safeguards and security deficiencies.

(c) Approve all Site Safeguards and Security Plans, and participate in validation and verification reviews at field sites.

(d) Establish and maintain the DOE Declassification Program and ensure consistency between classification and safeguards and security policies.

(e) Serve as DOE's central point for coordination and liaison with other agencies, groups, and DOE Elements in the development and execution of an effective Safeguards and Security Program.

(f) Coordinate with DOE Elements in the recommended curtailment or suspension of operations at DOE facilities when continuation of such operations would result in an ↩**unacceptable risk**↪ to national security, the health and safety of employees, the public, or the environment. Suspend the facility clearance where the level of the facility's safeguards and security program has significant vulnerability, ↩**unacceptable risk**↪, or inadequate protection, and approve removal of facility clearance. Reinstate facilities when satisfactory conditions exist. Notify other Federal agencies having concurrent safeguards or security interests of suspension or reinstatement actions.

(g) Advise Program Offices on their safeguards and security requirements and budgets before DOE approval. Ensure differences identified through the review process are resolved during DOE's internal review budgeting process (or equivalent process for reprogramming actions).

(h) Through the Director of Safeguards and Security.

1 Serve as the DOE focal point for safeguards and security matters.

2 Formulate policies, procedures, and plans to ensure the effective and efficient protection of nuclear materials, classified information, and DOE property and facilities.

a Base policies, procedures, and plans on the design basis threat requirements, standards, and guidelines.

b Provide, as requested, advice and assistance to Secretarial Officers and Heads of Field Elements in the implementation of safeguards and security requirements.

c Act as DOE's focal point for the collection, retention, evaluation, and dissemination of information of safeguards and security significance, including threat assessment and protection systems data.

d Develop and maintain guidelines for Site Safeguards and Security Plans, in consultation with affected DOE Elements.

e Establish safeguards and security policy and training quality panels.

f Approve or disapprove exceptions in accordance with paragraph 4f(3(a) to (e).

3 Provide focus for interagency matters pertaining to safeguards and security, including wartime protection planning and law enforcement; provide liaison with the Nuclear Regulatory Commission, Federal Bureau of Investigation, Department of Defense, and other Federal law enforcement and security agencies.

4 Recommend suspension of the facility clearance of any facility whose safeguards and security program is unacceptable in meeting minimum safeguards and security protection levels and associated risk.

5 Direct the safeguards and security technology development program to support user needs and policy objectives.

6 Participate in staffing line-item construction project actions for prioritizing projects through validation of specific projects and participate in program office Change Control Board actions.

7 Consolidate and coordinate the Annual Report to the Secretary on the Safeguards and Security Status.

8 Ensure development, conduct, and management of an effective Safeguards and Security Training Program.

a Develop and issue policy for safeguards and security training programs and coordinate with the Assistant Secretary for Human Resources and Administration to ensure conformance with DOE training policy. b Provide and manage personnel standardized training program at the Safeguards and Security Central Training Academy.

c Ensure that a safeguards and security Training Approval Program is developed, implemented, and administered.

d Conduct annual reviews of safeguards and security training programs DOE-wide and report findings as part of the annual report to the Secretary.

e Approve certifications that local safeguards and security training programs meet DOE standards.

9 Ensure the development, implementation, and management of an effective Safeguards and Security Awareness Program.

10 Oversee implementation of the Classified Visits Program.

a Obtain and review security assurances to determine consistency with agreements for cooperation and other international agreements, when applicable.

b Maintain a current list of all Department of Defense and National Aeronautics and Space Administration officials authorized to certify personnel under their jurisdiction for access to Restricted Data, and provide such lists to DOE Elements.

c Help identify Heads of DOE Elements and Federal officials to whom specific requests for visits should be directed.

d Approve requests for classified visits involving safeguards and security programmatic matters.

e Certify on DOE F 5631.20, "Request for Visit or Access Approval," the DOE access authorization type, number, and date for individuals possessing a DOE Headquarters access authorization in those instances in which this form is required.

11 Maintain the Safeguards and Security Information Management System.

12 Ensure the development, implementation, and management of an effective Facility Survey and Clearance Program.

a Designate a trained Facility Survey and Clearance Program Manager (a DOE employee).

b Approve extended survey schedules for facilities with Category I quantities of special nuclear material.

13 Ensure the development, implementation, and management of an effective FOCI.

a Designate a trained FOCI Program Manager (a DOE employee).

b In coordination with General Counsel, when appropriate, provide a favorable FOCI determination to the Lead Responsible Office.

14 Through the Director of Safeguards and Security Central Training Academy, manage the Academy to achieve program objectives expressed in Chapter II.

15 Through the Director, New Brunswick Laboratory.

a Manage the Laboratory to achieve program objectives.

b Provide state-of-the-art services for measurement of nuclear materials in support of DOE safeguards requirements.

c Assess the effectiveness of DOE facility materials measurement processes and materials control and accountability programs.

d Provide certified reference materials ensuring traceability of DOE nuclear materials measurements to a national and international measurements data base.

(i) Through the Director of Declassification, arrange and approve classified visits of foreign nationals sponsored by a foreign government to the Office of Declassification in connection with the information classification programs, and refer security assurances to the Office of Safeguards and Security.

(2) Through the Director of Energy Intelligence.

(a) Appoint a Special Security Officer for line management security administration of DOE's Sensitive Compartmented Information Facilities.

(b) Provide accreditations, in coordination with the Office of Safeguards and Security, that planned/installed physical and technical security systems create an environment of acceptable risk for intelligence-related facilities.

(c) Serve as DOE's point-of-contact involving intelligence and counterintelligence activities, to include management of program access. Coordinate with the Director of Security Affairs concerning security issues, including espionage and the potential compromise of intelligence-related information.

(3) Through the Director of Emergency Management, provide timely and current intelligence threat information to support the Safeguards and Security Program.

c. The Assistant Secretary for Environment, Safety and Health, through the Deputy Assistant Secretary for Oversight.

(1) Maintain an inspection, performance testing, and evaluation program that, in accordance with DOE 5630.12A, SAFEGUARDS AND SECURITY INSPECTION AND ASSESSMENT PROGRAM, provides independent oversight of the Department's Safeguards and Security Program.

(2) Ensure participation with the Department of Defense in conducting joint ATOMAL inspections to verify that Restricted Data and Formerly Restricted Data released by the United States to NATO and NATO member nations as ATOMAL information is being protected appropriately.

(3) Ensure all NATO/ATOMAL Control Points and Subcontrol Points are inspected to verify NATO and ATOMAL holdings are being appropriately protected.

d. Assistant Secretary for Defense Programs shall, in addition to the responsibilities in paragraph 5a, support the Classified Visits Program by appointing an approval authority for requests for visits requiring access to the following:

(1) Nuclear weapon information concerned with the design, manufacture, or use of atomic weapons, atomic weapon components, or atomic explosive devices; and nuclear weapon information in connection with the military application of atomic energy under sections 144b and c(1) and 91(c) or (4) of the Atomic Energy Act of 1954, as amended. (NOTE: Approval authority will be responsible for obtaining endorsements for programmatically controlled access for specific nuclear weapon information.)

(2) Nuclear materials production facilities or access to sensitive nuclear materials production information, excluding classified uranium enrichment technology .

(3) Classified production facilities, excluding visits for classified uranium enrichment technology, by employees of other Federal agencies, their contractors, or subcontractors.

e. Assistant Secretary for Human Resources and Administration shall establish programs and training for communications security, electronic emissions control (emissions security), and unclassified computer security.

f. Deputy Assistant Secretary for International Energy Policy shall serve as approval authority, in concert with appropriate Headquarters program staff, for classified visits by foreign nationals.

g. Associate Deputy Secretary for Field Management.

(1) Ensure strategic planning is completed for all Field Elements and conduct management coordination and oversight of multi-purpose Operations Offices as they impact the Safeguards and Security Program planning process.

(2) Ensure requirements for physical protection of facilities are incorporated into construction contracts.

h. The Director, Office of Nuclear Energy, through the Director of Uranium Programs, shall approve requests for visits involving access to uranium enrichment plants and to facilities engaged in uranium enrichment technology development, including gaseous diffusion, gas centrifuge, and advanced isotope separation technologies. (Managers of Field Elements may approve visits to facilities under their jurisdiction for contractors requiring access because of their continuing programmatic association or for contractor personnel administered under contracts with the Field Elements.)

i. Director, Naval Nuclear Propulsion Program, shall implement and oversee all policy and practices pertaining to this Order for activities under the Director's cognizance.

j. Heads of Field Elements shall ensure that all operations under their jurisdiction are implemented consistent with acceptable safeguards and security practices and in accordance with the Safeguards and Security directives.

k. Albuquerque, Chicago, Idaho, Nevada, Oak Ridge, Richland, Oakland, and Savannah River Operations Offices; Pittsburgh and Schenectady Naval Reactors; Rocky Flats Office; Strategic Petroleum Reserve Office; and the Office of Safeguards and Security, Headquarters Operations Division.

(1) Lead Responsible Offices.

(a) Ensure safeguards and security surveys of facilities under their purview are conducted.

(b) Establish written delegations of authorities and responsibilities for administration of the facility survey, registration and clearance, and FOCI programs.

(c) Designate a Facility Clearance Operations Manager (DOE employee) to manage the local program.

(d) Designate a FOCI manager (DOE employee) to manage the local program.

(e) Ensure the designation of a trained DOE employee as the FOCI point of contact in each contracting/procurement organization.

(f) Ensure the designation of a trained DOE employee as the FOCI point of contact in the Chief Counsel office.

(g) Develop local implementing procedures for the facility survey, registration and clearance, and FOCI programs.

(h) Grant approval for facilities and register safeguards and security activities.

(i) Terminate facility clearances and registrations of safeguards and security activities under their cognizance.

(j) Maintain information in the Safeguards and Security Information Management System for all facilities for which they are either the Lead Responsible Office or at which they have registered a safeguards and security activity.

(k) Ensure affected Departmental Elements are notified when an activity is suspended or terminated.

(l) Provide written notification to an approved facility whenever there is a change in the Lead Responsible Office.

(2) Surveying Offices.

(a) Ensure that an effective program is instituted to plan, conduct, and follow up safeguards and security surveys and self-assessments.

(b) Designate a Facility Survey Operations Manager (a DOE employee).

(c) Develop local implementing procedures for the administration and conduct of surveys and self-assessments.

(d) Provide input to the Safeguards and Security Information Management System current data for all surveyed facilities.

(e) Provide sufficient resources for the survey program to support professional, administrative, technical, and clerical staffing requirements, equipment and materials, logistics requirements, and training and development.

(f) Ensure that prior to working independently, persons assigned to perform survey and review duties possess appropriate knowledge, skills, and ability.

l. General Counsel.

(1) Appoint a trained DOE employee to serve as the FOCI point-of-contact.

(2) Upon request by the Office of Safeguards and Security, ensure review of all complex FOCI cases; e.g., FOCI cases involving Proxy Agreements and Voting Trusts.

m. Procurement Request Originators are the individuals responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization," or such other individuals(s) as designated by cognizant Heads of DOE Elements. Procurement Request Originators shall notify the cognizant contracting officers of the following:

(1) Each procurement requiring the application of this Order.

(2) Requirements for flow-down of this Order to any subcontract or subaward.

(3) Identification of the paragraphs or other portions of this Order with which the awardee or, if different, a subawardee is to comply.

n. Contracting Officers at all levels shall:

(1) Incorporate contract provisions implementing the applicable requirements of Safeguards and Security directives in new or existing contracts, and

(2) Not award contracts requiring access authorizations until a Facility Clearance is granted.

6. CONTACT. Comments and inquiries may be directed to the Materials Control and Accountability Program Manager, 301-903-2536, or to the points of contact provided in the chapters.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

TABLE OF CONTENTS

Page

CHAPTER I - SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. Objective. I-1
2. Applicability. I-1
3. Planning Requirements. I-1
4. Planning I-3
5. Implementation Assistance. I-5
6. Contact. I-5

CHAPTER II - SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. Objective. II-1
2. Applicability. II-1
3. Program Requirements II-1
4. Contact. II-4

CHAPTER III - PERFORMANCE ASSURANCE PROGRAM

1. Objective. III-1
2. Applicability. III-1
3. Program Requirements III-1
4. Documentation Requirements III-1
5. Contact. III-2

CHAPTER IV - SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. Objective. IV-1
2. Applicability. IV-1
3. Program Requirements IV-1
4. Documentation Requirements IV-3
5. Contact. IV-3

CHAPTER V - FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. Objectives V-1

2. Applicability. V-1
3. Requirements: General V-1
4. Requirements: Lead Responsible Office V-2
5. Requirements: Safeguards and Security Information Management SystemV-2
6. Requirements: Facility Clearances. V-3
7. Requirements: Facility Data and Approval Record. V-6
8. Requirements: Activity Registration. V-7
9. Requirements: Contract Security Classification SpecificationV-8
10. Requirements: Facility Importance Ratings. V-8
11. Implementation Assistance V-8
12. Contact V-8

CHAPTER VI - FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. Objective VI-1
2. Applicability VI-1
3. Requirements. VI-1
4. Eligibility Requirements. VI-3
5. Requirements: Processing Contractors for FOCI DeterminationsVI-4
6. Requirement: Accepting a FOCI Determination Rendered by Another Federal Agency VI-5
7. Requirements: Schedule of Requirements for Processing FOCI Determinations. VI-5
8. Requirements: Significant Changes. VI-6
9. Requirements: Adverse Determination. VI-7
10. Requirements: Methods to Negate or Reduce Unacceptable FOCIVI-7
11. Requirements: Methods to Negate or Reduce Risk in Foreign Ownership Cases. VI-7
12. Requirements: Annual Reviews and Compliance. VI-12
13. Contact VI-13

CHAPTER VII - INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. Objectives. VII-1
2. Applicability VII-1
3. Requirements. VII-2
4. Contact VII-3

CHAPTER VIII - CONTROL OF CLASSIFIED VISITS PROGRAM

1. Objectives. VIII-1
2. Applicability VIII-1
3. Requirements: Classified Visit Procedures. VIII-1
4. Requirements: Classified Visits by DOE Employees, Contractors and SubcontractorsVIII-2
5. Requirements: Visits to Department of Defense and National Aeronautics and Space Administration Facilities VIII-3
6. Requirements: Restricted Data Visits by Nuclear Regulatory Commission and Employees VIII-3
7. Requirements: Restricted Data Visits by Department of Defense and National Aeronautics and Space Administration Employees. VIII-4
8. Requirements: Other Classified Visits by Department of Defense and National Aeronautics and Space Administration Employees. VIII-5
9. Requirements: Classified Visits by Employees of Other Federal AgenciesVIII-5
10. Requirements: Congressional and State Classified VisitsVIII-5
11. Requirements: Emergency Visits to Classified Areas and FacilitiesVIII-6
12. Requirements: Classified Visits by Foreign Nationals to DOE FacilitiesVIII-6
13. Contact VIII-6

Attachment VIII-1 - Access to Restricted Data in Possession of Other Federal AgenciesVIII-7

CHAPTER IX - SURVEY PROGRAM

1. Policy/Objectives IX-1
2. Applicability IX-1
3. Types of Surveys. IX-1
4. Scope of Surveys. IX-2
5. Requirements: Frequency of Surveys IX-2
6. Requirements: Survey Conduct IX-4
7. Requirements: Survey Reports IX-5
8. Requirements: Rating System. IX-6
9. Reporting Requirements: Marginal and Unsatisfactory Composite RatingsIX-7
10. Requirements: Corrective Actions IX-9
11. Contact IX-10

CHAPTER X - SELF-ASSESSMENT PROGRAM

1. Objective X-1
2. Applicability X-1
3. Requirements. X-1
4. Contact X-2

CHAPTER I

SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a standardized approach to protection program planning that will provide an information baseline for use in integrating complex-wide safeguards and security considerations, facilitate managers' evaluation of program elements and resources for needed improvements, and establish cost-benefit bases for analyses and comparisons.

2. APPLICABILITY. This chapter applies to the following DOE-owned and -leased sites and facilities and to covered contractor-owned and -leased facilities.

a. Those that have Category I quantities of special nuclear materials, or those that have Category II quantities within the same Protected Area that roll up to a Category I quantity.

b. Those that have a radiological/toxicological sabotage threat that would cause an unacceptable impact on the national security, the health and safety of employees, the public, or the environment.

c. Those that have an industrial sabotage threat that would cause an unacceptable impact to those DOE programs supporting national defense and security.

d. Those facilities engaged in intra-site transportation of special nuclear materials.

e. Those facilities possessing classified matter.

f. Those facilities engaged in the protection of government property.

g. Other facilities/sites that Heads of DOE Elements deem appropriate.

3. PLANNING REQUIREMENTS. The following topics shall be essential elements for planning safeguards and security programs.

a. Site-Specific Characteristics. Protection programs shall be tailored to address specific site

characteristics and requirements, current technology, ongoing programs, and operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis.

b. Threat. The "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall be used with local threat guidance and vulnerability assessments for protection and control program planning.

c. Protection Strategy.

(1) Strategies for the physical protection of special nuclear materials and vital equipment shall incorporate the applicable requirements established in DOE M 471.2, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.

(a) Protection strategy may be graduated to address varying circumstances and may range from denial to containment to recapture/recovery to pursuit.

(b) A denial strategy shall be used for the protection of Category IA special nuclear materials and certain radiological sabotage targets where unauthorized access presents an **unacceptable risk**.

(c) Programs shall be designed to prevent unauthorized control (i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials for onsite assembly of an improvised nuclear device).

(d) A containment strategy shall be used to prevent the unauthorized removal of Category II or greater special nuclear materials.

(e) Should denial and/or containment fail, a recapture/recovery or pursuit strategy would then be required.

(f) Forces shall be capable of rapid reaction in implementing recapture or recovery contingencies.

(g) Programs must be designed to prevent acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment, and/or mitigate the consequences of acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

(2) Strategies for the protection and control of classified matter shall incorporate the applicable requirements established in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS; DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM; and DOE M 471.2-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM. Security systems shall be used that detect or deter unauthorized disclosure, modification, or the loss of availability of classified and sensitive, but unclassified, information and its unauthorized removal from a site or facility.

(3) Strategies for the protection of Government property not covered in subparagraphs (1) and (2) above shall reflect a graded approach.

(4) Security countermeasures to address bombings shall consider a range of activities from

hand-carried, mailed, and vehicle-transported devices.

d. Graded Protection. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

4. PLANNING.

a. Site Safeguards and Security Plan. This plan is an Operations Office or equivalent-level master planning document that shall be prepared for sites with facilities described in paragraphs 2a, 2b, 2c, and 2g. The plan shall depict the existing condition of safeguards and security sitewide and by facility, and shall establish improvement priorities and resource requirements for the necessary improvements. Plans shall contain information that describes:

(1) protection strategies;

(2) site/facility safeguards and security programs in place and/or planned;

(3) plans and procedures designed to implement, manage, and maintain safeguards and security programs;

(4) resources needed to sustain the site protection program in its current configuration and during planning revisions;

(5) security staff personnel qualifications as outlined in approved position descriptions and/or prescribed in DOE directives;

(6) the results of vulnerability analyses and risk assessments:

(a) levels of acceptable risks;

(b) assumptions established and used as part of the vulnerability assessment process;

(c) validation of vulnerability analyses results by performance testing;

(7) required corrective actions and how those actions will mitigate identified vulnerabilities and reduce residual risk;

(8) sources of supporting documentation detailing where planning assumptions, relative to the facility, the adversary, and the DOE national security mission can be found; and

(9) approved deviations.

b. Security Plans. At locations where a Site Safeguards and Security Plan is not required due to the limited scope of safeguards and security interests, a security plan shall be developed to describe the protection program in place. In addition, specialized plans shall be developed to address protection programs for classified automated information systems, materials control and accountability, and other protection operations. Requirements for specialized plans that may or may not be components of Site Safeguards and Security Plans are set forth in the applicable DOE O 470 and 5630 series of directives.

(1) Materials Control and Accountability Plans. See DOE 5633.3B, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 9-7-94, for requirements for this type of plan.

(2) Classified Automated Information System (AIS) Security Plans. See DOE M 5639.6A-1 for requirements for this type of plan.

c. Planning Inputs. The following documents shall be used to support program forecasts and information input used in the protection program planning process.

(1) Current DOE directives, DOE threat guidance, and applicable intelligence assessment information developed and disseminated by Headquarters Elements.

(2) Programmatic guidance and forecasts of significant changes planned in site operations, as communicated through Heads of Field Elements and appropriate Headquarters Elements.

(3) Current and projected operational constraints and resources.

(4) Protection program policy guidance provided by DOE Elements.

d. Plan Review and Approval.

(1) Heads of Field Elements shall approve and forward Site Safeguards and Security Plans to the applicable program office for coordination. Changes to the Plans that significantly alter the agreed-on protection philosophy or performance standards of protection systems shall require approval by the Head of the Field Element and concurrence by the cognizant program office and the Director of Security Affairs. Other plans shall be approved by the Head of Field Element or as stipulated in the applicable directive.

(2) The Site Safeguards and Security Plan shall be reviewed and updated annually. Copies of modifications and updates will be provided to the Office of Safeguards and Security for review and comment.

5. IMPLEMENTATION ASSISTANCE. The Office of Safeguards and Security will develop and maintain, after appropriate coordination with affected elements, guidelines to assist facilities in safeguards and security planning.

6. CONTACT. Comments and inquiries on this chapter may be directed to the Materials Control and Accountability Program Manager at (301) 903-2536. Inquiries pertaining to implementation may be directed to the Field Operations Division at (301) 903-4243.

CHAPTER II

SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. OBJECTIVE. To train DOE and DOE contractor personnel to a level of proficiency and competence that ensures they are qualified to perform assigned safeguards and security tasks and/or responsibilities, thus providing high assurance that the safeguards and security programs of the Department are successful.

2. APPLICABILITY. This chapter applies to personnel performing tasks and responsibilities addressed in this and other Safeguards and Security directives associated with protecting nuclear weapons, weapons components, special nuclear materials, classified matter, and/or government property.

3. PROGRAM REQUIREMENTS.

a. The Safeguards and Security Training Program shall encompass training in the following Safeguards and Security Program key elements.

(1) Program Management.

(2) Personnel Security.

(3) Protection Operations.

(4) Materials Control and Accountability.

(5) Information Security.

b. Training methodology and courses shall be standardized. The scope and level of training provided to individuals shall be tailored to their assigned duties and responsibilities and shall be based upon an analysis of their prior safeguards and security experience and training.

c. Training programs shall be based on the results of job analyses to document the identification and description of major tasks and skill requirements.

d. Knowledge and performance-based testing shall apply to all required training to measure the skills acquired from the training programs developed.

e. For specialized skill requirements, such as armorers, personnel security specialists, nuclear materials custodians, and technical surveillance countermeasures technicians, performance testing shall form the primary basis for certification.

f. The Training Approval Program (TAP) is a process to formally recognize safeguards and security training programs that are conducted by an organization other than the Safeguards and Security Training Academy to ensure established objectives, standards, and criteria are met.

(1) A Training Approval Program shall be implemented to ensure standardization of safeguards and security training conducted at DOE facilities other than the Safeguards and Security Central Training Academy. (The "Guide for Implementation of DOE 5630.15, Safeguards and Security Training Program" provides details on Training Approval Program implementation.)

(2) Developed and refined safeguards and security training program objectives, standards, and criteria shall be distributed to facilitate development of training programs.

(3) Site programs shall be examined by representatives of the Office of Safeguards and Security on a recurring basis, but no less than every 3 years, to verify adherence to DOE objectives, standards, and criteria, and to provide program approval recommendations to the Director of Safeguards and Security.

(4) Initial and recurring reviews for training approval shall cover all aspects of local training programs to include program management and structure, course contents, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(5) Instructors shall be evaluated for knowledge in their assigned training area and effectiveness in presenting assigned course materials.

(6) Individuals shall be tested to evaluate skills and knowledge achieved through course participation.

(7) Training approvals shall remain valid for a period of 3 years.

g. Training shall be provided to individuals to qualify or improve their qualifications to perform assigned safeguards and/or security tasks or responsibilities. Initial and refresher training shall be tailored to the required knowledge and skills.

h. The Safeguards and Security Central Training Academy shall provide a state-of-the-art training facility and program, emphasizing training for DOE Element instructors and instructor-candidates, as follows.

(1) Standardization of training in safeguards and security courses and programs through certification of key skill personnel, development of skills enhancement courses, and approval of facility training programs.

(2) Standardization of training courses for the key program elements. Information associated with these training courses would be available to DOE Elements and contractors for use in their training programs.

(3) Standardization of testing procedures to assess proficiency, knowledge, and skills. Associated information would be made available to DOE Elements and contractors.

(4) Development and maintenance of a repository of information pertaining to relevant external sources of training and training materials, as well as data regarding needs that cannot be satisfied by DOE resources.

(5) Maintenance of a library of current and historical reference materials to support all aspects of the training program.

(6) Effective relationships with other Federal training facilities and operational safeguards and security functions to further training objectives.

(7) Review of DOE and contractor safeguards and security training programs to assess adherence to established quality standards in course content and presentation.

i. A Safeguards and Security Training Advisory Committee shall be chaired by the Director of the Central Training Academy.

(1) Members shall include two senior level officials from the Office of Safeguards and Security, two senior officials from DOE Operations Offices who are nominated by the chair and approved by the Director of Safeguards and Security, and two senior contractor personnel to serve as technical advisors. Technical advisors shall be nominated by the chair and approved by the Director of Safeguards and Security. Members and technical advisors shall serve for 2 years or as decided by the Director of Safeguards and Security. The chair of the Committee shall hold meetings at least semi-annually.

(2) The Committee shall:

(a) review, evaluate, and recommend specific subject areas and curriculum content required to establish standardized training;

(b) recommend and assist in obtaining resources required to support the standardized training program;

(c) review the implementation status of safeguards and security training policy and guidance; and

(d) annually review and validate the Central Training Academy's operations, course schedule, course approval and certification procedures, and strategic plans.

j. Central Training Academy instructors shall be certified by the Director of the Academy.

(1) Certification shall remain valid so long as the individual fulfills all required refresher

training.

(2) Certification shall be based on a records review of qualifications and a recommendation by the individual responsible for the training program.

(3) Instructors of courses provided by other DOE Elements and contractors shall be certified by the individual responsible for the DOE Element or contractor training program.

k. Development, review, and presentation of training courses for unique site-specific requirements shall be the responsibility of cognizant sites. Course materials shall be available upon request for review and approval by the cognizant Departmental Element and/or the Training Approval Program team.

l. The Central Training Academy, DOE Elements, and covered contractors shall implement a standardized training records management system as described below.

(1) Records shall be maintained to document training provided to personnel participating in the DOE safeguards and security program. Records of training shall contain course identification, dates accomplished, and scores achieved where applicable.

(2) Records of training provided to individuals shall be retained in electronic or hard copy form. Records shall be retained according to guidance provided in DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95, and General Records Schedules issued by the Archivist of the United States.

(a) Records of training provided at the Central Training Academy shall be maintained at the Academy and shall also be maintained by the organization sponsoring the individual.

(b) Records of training provided at DOE Elements shall be maintained at DOE Headquarters or the relevant Operations Office, as appropriate, and shall be provided to the organization sponsoring the individual for inclusion in the individual's record file.

(c) Records of training provided at contractor facilities shall be provided to and retained by the organization sponsoring the individual.

(d) Records of training provided at other government or private facilities shall be obtained and maintained by the organization sponsoring the individual.

4. CONTACT. Comments and inquiries on this chapter may be directed to the Materials Control and Accountability Program Manager at (301) 903-2536.

CHAPTER III

PERFORMANCE ASSURANCE PROGRAM

1. OBJECTIVE. To demonstrate the effectiveness of the protection posture for Category I and Category II quantities that roll up to the Category I category of special nuclear material and Top Secret matter by systematically evaluating systems that provide essential protection measures.

2. APPLICABILITY. The program applies to safeguards and security systems and their essential components (e.g., equipment, hardware, administrative procedures, protective forces, personnel) that are used to protect Category I and II special nuclear materials and/or Top Secret matter.

3. PROGRAM REQUIREMENTS. Performance assurance shall be provided for systems and/or system components for those systems providing essential protection for Category I and Category II special nuclear material and/or Top Secret matter.

a. Performance assurance programs shall provide for operability and effectiveness tests of systems and/or components of systems. Systems and/or essential components of systems whose failure would reduce protection to an unacceptable level shall be tested at a frequency that provides high assurance of reliability for those systems and/or components. Testing frequencies shall reflect site-specific conditions, operational needs, and threat levels. Testing frequencies shall be documented.

(1) Operability tests provide a simple measure of integrity on a frequent basis. Operability testing shall consist of checking the system element or total system to confirm, without any indication of effectiveness, that it is operating.

(2) Effectiveness tests provide comprehensive assurance of integrity on an infrequent basis. Performance testing of equipment for effectiveness shall consist of checking systems to confirm the satisfactory performance of the required functions over the expected range of use.

b. The adequacy of new and existing protective systems shall be confirmed through testing prior to operational use and periodically thereafter.

c. At least every 365 days, a performance test encompassing protection systems associated with a comprehensive site or facility threat scenario shall be conducted to demonstrate overall facility safeguards and security system effectiveness.

4. DOCUMENTATION REQUIREMENTS.

a. Performance Assurance Program Plan. This plan may be an integral part of the Site Safeguards and Security Plan or other security plan, as applicable. The plan shall describe the program and its administration and implementation by:

(1) identifying protection elements for the protection of Category I and II special nuclear material and Top Secret matter;

(2) describing how the performance of these elements is to be ensured, including the manner in which activities performed by external oversight organizations will be applied and interpreted; and

(3) addressing unsatisfactory results of performance assurance activities, how they are to be captured in the site corrective action program, and how corrections will be implemented.

b. Performance Assurance Reports. Performance Assurance Reports shall be prepared to document results of implementation of performance assurance activities.

c. Document Retention.

(1) Recordkeeping systems shall provide an audit trail for performance assurance activities and reports.

(2) Disposition of documents shall be in accordance with DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95.

5. CONTACT. Comments and inquiries on this chapter may be directed to the Protection Operations Program Manager at (301) 903-4244.

CHAPTER IV

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. OBJECTIVES.

a. As a condition for access to classified information, special nuclear materials, and/or unescorted access to DOE Security Areas, excepting Property Protection Areas, individuals shall receive briefing(s). In addition, as a condition for access to classified information, individuals shall execute the Classified Information Nondisclosure Agreement.

b. Individuals shall be precluded or restricted from unescorted access to such DOE Security Areas and/or from access to classified information or special nuclear materials until the requirements of this chapter have been satisfied.

2. APPLICABILITY. A safeguards and security awareness program shall be developed, implemented, and maintained at each DOE and covered contractor site/facility having such DOE Security Areas, classified matter, and/or special nuclear materials.

3. PROGRAM REQUIREMENTS.

a. Safeguards and Security Awareness Coordinator. Each affected DOE Element shall appoint a Safeguards and Security Awareness Coordinator who shall ensure that the requirements of this Chapter are met.

b. Classified Information Nondisclosure Agreement. Prior to being granted access to classified information, individuals granted DOE access authorizations shall execute a Classified Information Nondisclosure Agreement. A refusal to execute the Classified Information Nondisclosure Agreement shall be grounds for the denial to classified information.

c. Briefings. Safeguards and security awareness programs shall include, but are not limited to, the development and presentation of four briefings:

(1) Initial Briefing.

(2) Comprehensive Briefing.

(3) Refresher Briefing.

(4) Termination Briefing.

Vertical line denotes change. d. Topics. Safeguards and security awareness programs shall incorporat information concerning the following:

(1) Applicable DOE safeguards and security, directives and procedures.

(2) Site-specific (and/or operations-specific) safeguards and security policies, procedures, and requirements.

(3) Other matters of safeguards and security interest, such as:

(a) recent espionage cases,

(b) approaches and recruitment techniques employed by foreign intelligence services,

(c) safeguards or security incidents and considerations, and

(d) safeguards or security threats and vulnerabilities.

c. Initial Briefing.

(1) Individuals approved for unescorted access to Security Areas (except Property Protection Areas) shall receive an Initial Briefing.

(2) Briefing topics shall include, but are not limited to:

(a) overview of DOE safeguards and security disciplines, to include personnel security, information security, and physical security;

(b) local access control procedures and escort requirements;

(c) protection of Government property;

(d) prohibited articles; and

(e) reporting of incidents of safeguards and security concern.

d. Comprehensive Briefing.

(1) Prior to being granted access to classified information or special nuclear materials, individuals granted DOE access authorizations shall receive a comprehensive briefing to inform them of their safeguards and security responsibilities. When such individuals are assigned to another DOE site, they shall receive comprehensive briefings at the new site.

Vertical line denotes change.

(2) Briefing topics shall include, but are not limited to, the following:

(a) Information Security.
(b) Physical Security.
(c) Personnel Security.
(d) Reporting/notification requirements.
(e) Legal and administrative sanctions imposed for incurring a security infraction or committing a violation.
(f) General information concerning the protection of special nuclear materials.

g. Refresher Briefings. Individuals who possess DOE access authorizations shall receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities. Refresher briefings are mandatory for all individuals possessing DOE access authorizations and shall be implemented each calendar year at approximately 12-month intervals.

h. Termination Briefings. Individuals shall receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing shall be implemented on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information or special nuclear materials, whichever is sooner. Termination briefings shall be based on the information contained in DOE F 5631.29, "Security Termination Statement," and the Classified Information Nondisclosure Agreement.

i. Manual. A Manual for this program shall be developed and maintained by the Office of Safeguards and Security for distribution to DOE Elements and covered contractors having DOE Security Areas, classified matter, and/or special nuclear materials to facilitate the implementation of this chapter.

4. DOCUMENTATION REQUIREMENTS.

a. Recordkeeping. Records shall be maintained to identify all individuals who have received briefings by type and date of briefing. Recordkeeping systems shall be capable of providing an audit trail.

b. Documentation.
(1) A completed Classified Information Nondisclosure Agreement may serve as documentation for the Comprehensive Briefing.
(2) In recurring requirements, such as the refresher briefing, records shall be maintained until the next occurrence of the briefing.
(3) The completion of DOE F 5631.29 satisfies documentation requirements for the termination briefing.

5. CONTACT. Comments and inquiries on this chapter may be directed to the Personnel Security Program Manager at (301) 903-3602.

Vertical line denotes change.

CHAPTER V

FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVES. To ensure proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment are afforded safeguards and security activitie

2. APPLICABILITY. This chapter applies to DOE Elements and personnel performing safeguards and security tasks and responsibilities addressed in this chapter and in other Safeguards and Security directives.

3. REQUIREMENTS: GENERAL.

a. Nuclear and other hazardous materials presenting a potential radiological or toxicological sabotage threat, classified matter, and property protection interests shall not be permitted on premises occupied by the Department or its contractors until facility clearance is granted.

b. Safeguards and security activities involving access authorizations shall be registered to assist in ensuring proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

c. If no need exists for a contractor's office locations to receive, process, reproduce, store, transmit, or handle classified information or nuclear material, but access authorizations are required for the contractor to perform the work within DOE-approved facilities, the contractor (identified as a non-possessing facility) must be cleared. As used in this Order, the term facility clearance refers to both possessing and non-possessing facilities.

d. Facility clearance shall be based upon a determination that satisfactory safeguards and security measures can be afforded the safeguards and security activities. The determination of a valid facility clearance shall be based upon an approved safeguards and security plan, results of surveys, and a favorable FOCI determination, as appropriate.

e. Approval for other Federal agency safeguards and security activities to be conducted at Department-owned or -operated facilities shall be based upon a determination that the safeguards and security measures to be provided are consistent with Departmental policy. Before acceptance of non-DOE safeguards and security activities, the Department and the requesting agency shall exchange appropriate classification and protection information. The exchange shall be documented in an agreement, which shall include appropriate reimbursement for safeguards and security costs incurred by the Department.

f. Facility clearance for work for others safeguards and security activities at other than Department-owned or -operated facilities that are channeled through a Departmental entity shall

be based upon validation of the other agency's facility clearance.

(1) Before commencement of non-DOE funded work, conduct, as required by DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, a review of the work request and certify that the sponsoring organization has either provided the appropriate classification guidance or has stated in writing that the non-DOE funded work will not entail classified activities.

(2) Ensure, prior to commencement of the non-DOE funded work involving access authorizations, that safeguards and security activities have been recorded as security interests on DOE F 5634.2 or DD F 254, "Contract Security Classification Specification."

(3) Ensure, before acceptance of any work for another Federal agency, that appropriate reimbursement for safeguards and security costs is negotiated.

4. REQUIREMENTS: LEAD RESPONSIBLE OFFICE.

a. The Lead Responsible Office grants facility clearance for eligible facilities under its cognizance.

b. If more than one Departmental Element has a registered activity at a facility, the organization responsible for the activity involving the highest classification level and category of activity is normally the Lead Responsible Office. However, this responsibility may, by mutual agreement, be accepted by a Responsible Office that does not have the highest classification level and category of activity, but has a greater scope of activity, such as with long term or traditional interests.

c. Any change in the Lead Responsible Office must include a transfer of appropriate documentation (e.g., safeguards and security plans, FOCI case files, status of unresolved findings).

d. Ensure safeguards and security surveys are accomplished using either internal assets or through a Memorandum of Understanding with another Surveying Office.

5. REQUIREMENTS: SAFEGUARDS AND SECURITY INFORMATION MANAGEMENT SYSTEM. Surveying and Lead Responsible Offices shall maintain information in the Safeguards and Security Information Management System for facilities over which they have responsibility, survey cognizance, or registered safeguards and security activities.

a. The Safeguards and Security Information Management System shall reflect facility information, activity information, and survey information.

b. Changes shall be accurately recorded and coordinated with the Lead Responsible Office in a timely manner.

c. Lead Responsible and Surveying Offices shall ensure that the Safeguards and Security Information Management System maintained at the Office of Safeguards and Security reflects established facilities and safeguards and security activities, under their jurisdiction, via prompt submission of accurate DOE F 5634.3 and DOE F 5634.2 and shall periodically review the Safeguards and Security Information Management System database to confirm the information contained therein is accurate.

6. REQUIREMENTS: FACILITY CLEARANCES. Facility clearances are recorded by Lead Responsible Offices, on DOE F 5634.3, "Facility Data and Approval Record" (see paragraph 7 of this chapter).

a. Granting Approval. Approval of a facility is based on the following:

(1) A favorable foreign ownership, control, or influence determination, in accordance with Chapter VI.

(2) A Facility National Agency Check, which has been requested or completed on those facilities that do not possess a Department of Defense (DOD) facility clearance, in accordance with Chapter VI.

(3) For contractors, contract(s) containing appropriate security clauses.

(4) Approved safeguards and security plans, as appropriate.

(5) If nuclear materials are involved, an established Reporting Identification Symbol code for Nuclear Materials Management and Safeguards System reporting.

(6) For the facility to possess classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or over $5,000,000 of DOE property, not including facilities or land values, at its location, an initial survey or other survey resulting in a report that comprehensively addresses the security interest, conducted no more than 6 months before the facility clearance date, with a composite facility rating of satisfactory.

(7) Appointment of a Facility Security Officer and, if applicable, Materials Control and Accountability Representative. The Facility Security Officer must possess a access authorization equivalent with the facility clearance.

(8) Access authorizations for appropriate personnel. Key management personnel must be determined case by case. The Lead Responsible Office FOCI Operations Manager, in conjunction with the Facility Clearance Operations Manager, is responsible for determining an organization's key management personnel. Key management personnel must possess access authorizations equivalent with the level of the facility clearance. Other officials, to be determined by the Lead Responsible Office, must possess appropriate access authorization for classified information or special nuclear materials.

b. Accepting a Contractor's Existing Federal Agency Facility Clearance. A contractor holding facility clearance from another Federal agency may be approved by DOE for processing, using, or storing classified matter, contingent on the following.

(1) The Federal agency facility clearance is at the appropriate classification level and encompasses the DOE activity. The other Federal agency's facility clearance shall not be accepted if it is based on a Special Security Agreement, Security Control Agreement, Limited Facility Clearance, or Reciprocal Clearance.

(2) The cognizant Federal agency agrees that it shall not cancel the facility clearance without prior notification to the Lead Responsible Office.

(3) The last survey report is acceptable in those areas that could affect the DOE activity.

(4) The cognizant Federal agency agrees to furnish the Lead Responsible Office copies of its periodic survey reports or memoranda covering the DOE activity.

(5) Each employee to be granted access to DOE classified information has, as a minimum, a Federal security clearance equivalent to that required by DOE, or reconciliation through interagency coordination on a case-by-case basis.

(6) If Restricted Data (RD) or Formerly Restricted Data (FRD) are involved, the cognizant Federal agency has provided assurance of compliance with the requirements of the Atomic Energy Act of 1954, as amended, including the mandatory personnel clearance

requirements.

(7) The requirements identified above have been documented in a letter or memorandum of agreement between the Lead Responsible Office and the cognizant Federal agency.

c. Verification of Federal Agencies. Verification of the capability of another Federal agency is based on written assurance from that agency that:

(1) classified matter shall be afforded protection according to Executive Order 12958, "National Security Information," and its implementing Information Security Oversight Office directives; and

(2) the requirements of the Atomic Energy Act of 1954, as amended, pertaining to access to Restricted Data and Formerly Restricted Data, including the mandatory personnel clearance requirements, shall be met.

When Restricted Data or Formerly Restricted Data is involved, this written assurance shall include coordination and reconciliation procedures to limit the manner in which this data is to be disseminated.

d. Suspension of Facility Clearance. The facility clearance for a contractor determined to be under FOCI shall be suspended pending final resolution and implementation of the security measures required to negate or reduce the foreign involvement. The contractor shall also be advised that failure to adopt required security deemed appropriate pending final resolution, may result in termination of its facility clearance. When findings or other deficiencies indicate suspension of a facility clearance is necessary, the responsible Head of Departmental Element, in coordination with the Office of Safeguards and Security, as appropriate, may suspend the facility clearance pending validated corrective actions. Once a decision is made to suspend the facility clearance, all affected Departmental Elements shall be notified by the Lead Responsible Office. The contractor subject to suspension action shall be notified that its facility clearance has been suspended, that performance on existing classified contracts may continue unless notified by DOE to the contrary, and that the award of new classified contracts will not be permitted until that facility clearance has been restored to a fully valid status.

e. Reinstatement. Following a survey to validate that corrective actions have been accomplished that restore a facility's safeguards and security posture to a composite satisfactory facility rating, the facility clearance may be reinstated. The Lead Responsible Office must complete a DOE F 5634.3 to enact the reinstatement.

f. Terminating Approval. When a facility has completed all safeguards and security activities involving work requiring access authorizations, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, classified matter, or over $5,000,000, exclusive of facility and land values) of Departmental property, the Lead Responsible Office shall ensure (1) a termination survey, as identified in Chapter IX, is conducted to verify appropriate disposition, destruction, or return of classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or Departmental property to DOE custody and (2) termination of all affected access authorizations. The Lead Responsible Office shall then terminate the facility clearance.

When a facility has been determined to have significant unresolved deficiencies or is under FOCI, the primary consideration shall be the safeguarding of classified information and/or special nuclear material. The Lead Responsible Office is responsible for taking whatever interim action it believes necessary to safeguard classified information and/or special nuclear material, in coordination with other affected DOE offices as appropriate. If the facility does not have possession of classified information and/or special nuclear material, and does not have a current or impending requirement for such access, the facility clearance shall be terminated. If final agreement by the parties with regard to the security measures to resolve deficiencies or to

negate or reduce the foreign involvement to an acceptable level, as determined by DOE, are not attained within a prescribed period of time, the facility clearance shall be terminated.

/. REQUIREMENTS: FACILITY DATA AND APPROVAL RECORD.

a. Purpose. The Facility Data and Approval Record is used to register pertinent facility information on the Safeguards and Security Information Management System. The Lead Responsible Office shall record a single DOE F 5634.3 to reflect the highest approved safeguards and security activity. Prompt entry on the Safeguards and Security Information Management System and accuracy of reported information are essential to the continued integrity of the safeguards and security program.

b. Preparation. A DOE F 5634.3 shall be prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental safeguards and security organization. Upon receipt, the responsible Operations Office safeguards and security organization or the Office of Safeguards and Security shall evaluate, survey, and approve the facility based upon an approved safeguards and security plan, safeguards and security surveys with a composite rating of satisfactory, and, if appropriate, a favorable FOCI determination.

(1) If a subcontract is established between a DOE prime contractor and another contractor for work involving access authorizations, classified matter, or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, it is the responsibility of the prime contractor to ensure proper preparation of a DOE F 5634.3.

(2) The Contracting Officer's Representative shall be responsible for validating information on the initial and subsequent DOE F 5634.3 and forwarding the form to the responsible DOE safeguards and security organization for approval.

c. Approval. DOE F 5634.3 shall be approved by the Lead Responsible Office.

d. Registration. The DOE F 5634.3, "Facility Data and Approval Record," must be completed by the Lead Responsible Office in order to register:

(1) facility clearance;

(2) a significant change in a facility (e.g., a change in name, address, Lead Responsible Office, classified mailing/shipping address, nuclear materials categorization, or classification level and category of information authorized);

(3) facility clearance termination;

(4) suspension of a facility clearance; or

(5) reinstatement of a suspended facility clearance.

e. Attachments. A copy of the facility's safeguards and security plan(s), survey report(s), and pertinent correspondence shall be maintained with DOE F 5634.3 for facility clearance. For facility termination a copy of the certificate of non-possession must be maintained.

8. REQUIREMENTS: ACTIVITY REGISTRATION. Activity registration is recorded on DOE F 5634.2, "Contract Security Classification Specification." (See paragraph 9 of this chapter.)

a. Accepting Existing DOE Facility Clearance.

(1) A Departmental Element seeking to establish an activity shall check the Safeguards and Security Information Management System to determine whether the contractor or prospective contractor currently holds a facility clearance. In coordination with the Lead

Responsible Office, an organization may accept the existing facility clearance, provided:

(a) the new activity shall be protected adequately under the facility's existing safeguards and security program as outlined in the applicable, approved safeguards and security plan;

(b) the existing facility clearance is compatible with the level of the new activity; and

(c) the facility holds a composite facility rating of satisfactory on the basis of the last safeguards and security survey report.

(2) When an activity will exceed the current facility clearance or a facility clearance does not exist, the actions required in paragraph 6 must be completed, as appropriate. The upgrading of a facility clearance may also require the transfer of the functions of the Lead Responsible Office.

b. Suspension of an Activity at a Facility. When current deficiencies indicate to responsible management officials that suspension is necessary for a specific activity, the Departmental Element establishing an activity, in coordination with the Lead Responsible Office, may suspend the activity and the ability of the facility to accept new safeguards and security activities pending correction of those deficiencies and validation of those corrective actions.

c. Reinstatement. Upon completion of a survey that validates corrective actions, the suspended activity may be reinstated. A DOE F 5634.2 is required to enact the reinstatement.

d. Terminating an Activity at a Facility. When a registered activity is terminated at an approved facility, the organization that established the activity must ensure that all affected access authorizations are terminated, and all nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, DOE property, and/or classified matter is appropriately reallocated, disposed of, destroyed, or returned to an appropriate organization. A certificate of non-possession shall be obtained from the Lead Responsible Office and maintained by the organization that established the activity.

9. REQUIREMENTS: CONTRACT SECURITY CLASSIFICATION SPECIFICATION.

a. New Activity. If a new activity for work involving access authorizations is being considered, the DOE F 5634.2 (or the DD F 254, Contract Security Classification Specification) must be submitted by the procurement request originator, to the Contracting Officer's Representative. These forms are used to register pertinent activity information on the Safeguards and Security Information Management System. The Contracting Officer's Representative shall validate the information on the DOE F 5634.2 (or DD F 254) and forward the form to the responsible DOE safeguards and security organization for approval.

b. Preparation. A DOE F 5634.2 shall be initially prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental Element Safeguards and Security organization. If a DD F 254, "Contract Security Classification Specification," has been used by the agency sponsoring the activity, it shall be annotated with the facility code and submitted instead of the DOE F 5634.2.

10. REQUIREMENTS: FACILITY IMPORTANCE RATINGS. Importance ratings shall be used to identify relative importance of facilities on the Safeguards and Security Information Management System and to determine survey frequency. A detailed explanation of these ratings is located in the Safeguards and Security Survey and Self-Assessment Guide.

11. IMPLEMENTATION ASSISTANCE. The Office of Safeguards and Security will develop an implementation plan for the implementation of DOE F 5634.2 and DOE F 5634.3 in the Safeguards and Security Information Management System. This implementation plan will be provided to each Lead Responsible Office and Survey Office, who shall use this plan to develop

a local implementation plan.

2. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. OBJECTIVE. It is DOE policy to obtain information that indicates whether offerors/bidders or contractors are owned, controlled, or influenced by a foreign person and whether as a result the potential for an undue risk to the common defense and national security may exist.

2. APPLICABILITY. Foreign ownership, control, or influence (FOCI) determinations are required of the following.

a. Contractors, which include any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government for the purpose of performing under a contract, license, or other arrangement that requires access authorizations. However, the foregoing does not include individuals performing work under a consulting agreement. This includes subcontractors of any tier, consultants, agents, grantees, and cooperative agreement participants.

b. All tier parents, if the contractor is owned or controlled by another firm(s).

3. REQUIREMENTS.

a. A favorable FOCI determination must be rendered on the prospective contractor and, if applicable, its tier parents, prior to the Lead Responsible Office granting a facility clearance or contract requiring access authorizations. Unless established thresholds are exceeded, the Lead Responsible Office shall render the FOCI determination(s) on the contractor and, if applicable, tier parents.

b. While the Lead Responsible Office will conduct a preliminary review of the FOCI representations and certifications of each firm in the competition range in a procurement request, a facility clearance, which requires a FOCI determination, can only be requested for the successful offeror/bidder if there is expected to be insufficient lead time between selection and contract award to allow deferral of the FOCI determination and facility registration.

c. Prior to the award of a contract requiring access authorizations to an offeror/bidder that does not possess a facility clearance, the offeror/bidder shall be required to submit to the Contracting Officer information and documentation that define the extent and nature of any foreign ownership, control, or influence over the offeror/bidder and, if applicable, its tier parents. The Contracting Officer cannot award the contract/agreement until he/she receives notification from the Lead Responsible Office that a favorable FOCI determination was rendered.

d. A contractor with a facility clearance is required to ensure that the following notification for its organization and each of its tier parents is immediately provided to the Lead Responsible Office.

(1) Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI representation and certification .

(2) Complete, current, and accurate information, certifications, and explanatory documentation that define the extent and nature of any relevant FOCI whenever:

(a) there is any change in ownership or control;

(b) 5 years have elapsed since the previously provided FOCI representations and certification were executed; or

(c) the Lead Responsible Office advises that it considers that a relevant change in the nature of the FOCI has occurred.

(3) Written notification of anticipated changes that include, but are not limited to, the following:

(a) action to terminate the contractor organization or any of its parents for any reason;

(b) imminent adjudication of or reorganization in bankruptcy of the contractor organization or any tier parents;

(c) discussions or consultations with foreign interests that may reasonably be expected to lead to the introduction or increase of FOCI; or

(d) negotiations for the sale of securities to a foreign interest that may lead to the introduction or increase of FOCI.

e. Contracting Officers must provide written notification to the servicing safeguards and security office in each of the following instances:

(1) A FOCI determination is required on an offeror/bidder and, if applicable, its tier parents. The Contracting Officers will send the servicing safeguards and security office the FOCI representations and certifications and supporting documentation, which have been reviewed for completeness.

(2) A requested FOCI review is no longer needed.

(3) A FOCI determination was rendered on an offeror/bidder that was not the successful bidder.

(4) Within 30 days of the termination or completion of all work by the contractor on a contract requiring access authorizations.

f. The Lead Responsible Office shall provide the successful offeror/bidder with written notification that:

(1) DOE has reviewed the FOCI submission and determined the organization is not under FOCI; or

(2) the contractor and any tier parents must keep the FOCI information current;

(3) identifies the Lead Responsible Office. This office is the only office to which the contractor and any tier parents will provide new FOCI representation and certification or written notification of anticipated or significant changes.

g. When established thresholds are exceeded, the Office of Safeguards and Security reviews FOCI cases submitted by a Lead Responsible Office to determine eligibility for a FOCI determination.

h. When a tier parent has not entered into a contract requiring access authorizations or is performing work on a contract requiring a lower level access authorization, the Lead Responsible Office shall obtain appropriate Board Resolutions from the contractor and its parent organization(s) to exclude the parent organization(s) from having any unauthorized

access.

If a contractor, offeror/bidder, and/or tier parent is determined to be under FOCI, the Lead Responsible Office shall ensure that the contractor is advised of the existence of FOCI and the security measures, if any that would be necessary to negate or reduce that foreign involvement and its effect.

j. When the offeror or bidder requiring access authorizations is a local, State, or Federal governmental agency or department, the affected contract must contain a security clause stating that if the governmental agency or department subcontracts any work requiring access authorizations to a commercial entity, their acquisition regulation, including FOCI policies will be followed. In the absence of their own FOCI policies, the DOE will render the FOCI determination.

k. To the extent permitted by law, information submitted in confidence as business/financial information shall be protected as Official Use Only, exempt from public release under the Freedom of Information Act.

4. ELIGIBILITY REQUIREMENTS. An organization will be considered under FOCI when a foreign person has the power, direct or indirect, whether or not exercised, and whether or not exercisable through ownership of the organization's and/or it tier parents' securities, through indebtedness, by contractual arrangements, or other means, to direct or decide matters affecting tl management or operations of that organization in a manner that may result in the compromise c classified information or unauthorized access to nuclear potential radiological or toxicological sabotage threat or of contracts requiring access authorizations. Eligibility r the following.

a. A organization effectively owned or controlled by a foreign government is ineligible for award of a contract if it is necessary for the organization to be given access to information in a proscribed category in order to perform the contract unless the foreign government ownership occurred prior to October 23, 1992. The Secretary of Energy may determine that a waiver from this requirement is essential to the national security interest of the U.S.

b. A organization that is owned, controlled, or influenced by a foreign person from a sensitive country identified in DOE 1500.3, FOREIGN TRAVEL AUTHORIZATION, of 11-10-86, and DOE 1240.2B, UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS, of 8-21-92 shall not be eligible, in some cases, for a favorable FOCI determination. The Office of Safeguards and Security will make the determination.

c. An organization that is owned, controlled, or influenced by a foreign person from a nonsensitive country shall be eligible for a favorable FOCI determination provided action can be taken to effectively negate or reduce associated FOCI risk to an acceptable level. The Office of Safeguards and Security will make the determination.

d. Key management personnel determined to require access authorizations, as set forth in Chapter V, paragraph 6a(8) must possess an access authorization to the level of the facility clearance.

5. REQUIREMENTS: PROCESSING CONTRACTORS FOR FOCI DETERMINATIONS.

a. The Contracting Officer will verify whether the offeror/bidder has a facility clearance through the Safeguards and Security Information Management System. If an offeror/bidder does not possess a facility clearance, the DOE contracting office shall request a complete FOCI package from the organization, and all tier parents. If the parent(s) has a facility clearance, a new FOCI package is not necessary. This package is reviewed for completeness by the DOE Contracting Officer and submitted to the servicing safeguards and security office.

b. Prior to a FOCI determination being rendered, the Lead Responsible Office must accomplish the following.

(1) Receive written confirmation of a contractor's facility clearance from the Defense Investigative Service (DIS)/Central Verification Activity (CVA). When the contractor has a Limited Facility Clearance (formerly "Reciprocal" clearance) or DIS/CVA cannot verify the contractor's clearance and provides a telephone number to call for verification, the FOCI submission must be immediately forwarded to the Office of Safegua Security for adjudication; or

(2) Request the Office of Safeguards and Security to obtain a Facility National Agency Check (FNAC) if the contractor does not have an active DOE or DOD facility clearance requiring access authorizations. However, the Lead Responsible Office can render the FOCI determination pending the results of the FNAC, under the following conditions.

(a) The responses to the FOCI questions do not exceed the thresholds established by the Office of Safeguards and Security.

(b) Exclusion procedures are invoked when the contractor requiring access authorizations is controlled by a parent(s) either not requiring access authorizations or requiring a lower-level access authorization.

(3) If the FOCI case exceeds established thresholds, the Lead Responsible Office shall forward the case file to the Office of Safeguards and Security with a recommended determination. Forwarded case files shall contain certifications from the offeror/bidder/contractor and any tier parents and shall document the reasons the case has been forwarded. The Office of Safeguards and Security shall review the package to determine if it concurs with the Lead Responsible Office's recommendation. The Office of Safeguards and Security, in coordination with General Counsel when appropriate, shall provide a final FOCI determination to the Lead Responsible Office.

6. REQUIREMENT: ACCEPTING A FOCI DETERMINATION RENDERED BY ANOTHER FEDERAL AGENCY. DOE will accept another Federal agency's FOCI determination when the requirements for accepting a facility clearance in Chapter V, paragraph 6b, are met.

7. REQUIREMENT: SCHEDULE OF REQUIREMENTS FOR PROCESSING FOCI DETERMINATIONS.

a. The Lead Responsible Office shall observe the following schedule in processing FOCI determinations.

(1) Initial review and verification procedures shall be accomplished within 15 working days of the receipt of a FOCI submission from the contracting officer.

(2) Within an additional 20 working days, one of the following actions will be taken.

(a) A FOCI determination will be rendered by the Lead Responsible Office if FOCI thresholds are not exceeded.

(b) If required, additional information, shall be requested either verbally or in writing from the offeror/bidder/contractor.

(c) The FOCI case, which has been reviewed for completeness, shall be forwarded to the Office of Safeguards and Security if established thresholds are exceeded.

b. For cases forwarded to the Office of Safeguards and Security for action, the foregoing

schedule shall also be observed.

c. If for any reason a FOCI determination has not been rendered within 90 working days of receipt:

(1) The Lead Responsible Office shall either (i) provide written notification to the submitting contracting officer with a copy to the Office of Safeguards and Security regarding the reason for the delay in processing/completing the submission or (ii) return the submission to the submitting contracting officer if the contractor has been non-responsive to the Lead Responsible Office's request for additional information or implementation or required security measures.

(2) The Office of Safeguards and Security shall either (i) provide written notification to the Lead Responsible Office regarding the reason for the delay in processing/completing the submission or (ii) return the submission to the Lead Responsible Office if the contractor has been non-responsive to the Office of Safeguards and Security's request for additional information or implementation of required security measures.

8. REQUIREMENTS: SIGNIFICANT CHANGES. When changes in the extent and nature of FOCI that would affect the information in a contractor's and/or any tier parents' most recent DOE FOCI submission(s) have occurred, the contractor/parent shall immediately provide written notification and supporting documentation relevant to the changes to the DOE Lead Responsible Office. A significant FOCI increase/change that warrants processing of the contractor/parent for a new FOCI determination includes, but is not necessarily limited to, the following.

a. A new threshold or factor that did not exist when the previous determination was made (e.g., a "no" answer changes to a "yes" answer), and any additional factors associated with the questions on the FOCI representation and certification.

b. A previously reported threshold or factor that was favorably evaluated by the Lead Responsible Office has increased to a level requiring a determination by the Office of Safeguards and Security.

c. A previously reported financial threshold or factor that was favorably evaluated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location of end user (i.e., for revenue and/or net income) or lenders (i.e., indebtedness).

d. A previously reported foreign ownership threshold or factor that was favorably evaluated by the Office of Safeguards and Security has increased to the extent that a method of negation or reduction (see paragraphs 10 and 11) is necessary.

e. Any changes in the ownership or control of the contractor and/or any tier parents.9. REQUI determined to be under FOCI will not implement the necessary security measures, as determined by DOE, to negate or reduce foreign involvement to an acceptable level, an adverse determination will be rendered by the Office of Safeguards and Security. When a contractor with a FOCI determination experiences significant changes in its FOCI resulting in a determination that the contractor is under FOCI, the contractor's facility clearance shall be suspended and may be terminated, as set forth in Chapter V, paragraphs 6d to f.

10. REQUIREMENTS: METHODS TO NEGATE OR REDUCE UNACCEPTABLE FOCI. The affected U.S. organization(s), or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however, DOE reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information and/or special nuclear materials is precluded. A plan may consist of one or more of the insulating measures prescribed in paragraph 11 as appropriate. It may also consist of other measures employed in conjunction with, or apart from, these methods, such as:

a. physical or organizational separation of the component performing the work requiring access authorizations,

b. modification or termination of agreements with foreign persons,

c. diversification or reduction of agreements with foreign persons,

d. diversification or reduction of revenue from foreign persons,

e. assignment of specific security duties and responsibilities to selected officials of the organization,

f. creation of special executive-level committees to consider and oversee classified information and/or special nuclear material.

11. REQUIREMENTS: METHODS TO NEGATE OR REDUCE RISK IN FOREIGN OWNERSHIP CASES.

a. National Interest Determination. An organization cleared under a Special Security Agreement and its cleared employees may only be afforded access to "proscribed information" with special authorization. This special authorization must be manifested by a favorable national interest determination that must be program/project/contract-specific. Access to proscribed information must be predicated on compelling evidence that release of such information to an organization cleared under the Special Sec security interests of the United States. Th permitted below the Assistant Secretary. determination will be prepared and sponso program, is involved and it shall include th

(1) Identification of the proposed awardee and a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action).

(2) General description of the procurement and performance requirements.

(3) Identification of national security interest involved and the ways in which award of the contract helps advance those interests.

(4) The availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract.

(5) A description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.

A national interest determination shall be initiated by the Contracting Officer. A company may assist in the preparation of the determination, but the Contracting Officer is not obligated to pursue the matter unless it believes further consideration to be warranted. The Contracting Officer shall, if it is supportive of the national interest determination, forward the case through appropriate channels. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required (e.g., NSA for COMSEC, DCI for SCI).

It is the responsibility of the cognizant approval authority to ensure that pertinent security, counterintelligence, and acquisitions interests are thoroughly examined.

b. Board Resolution for Noncontrolling Foreign Minority Cases. When a foreign person(s) owns

voting stock, directly or indirectly, but is not permitted representation in the U.S. organization (that is, to hold a position as or appoint any of the U.S. organization's management and/or allowed to transfer any of its employees on any of its foreign-owned parent's or other foreign-owned affiliate's employees to the U.S. organization), resolutions by the U.S. organization's board of directors and other actions as described below may be considered to negate or reduce the FOCI.

(1) Resolutions shall address the following.

(a) Acknowledge and describe all FOCI elements; identify foreign persons and describe the type and number of foreign-owned shares.

(b) Acknowledge the organization's obligations to comply with all security program and export control requirements.

(c) Certify that foreign persons shall not require, shall not have, and can be effectively precluded from access to all classified information or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat entrusted to or held by the U.S. organization; certify that the foreign persons will not be permitted representation in the U.S. organization or to influence the organization's policies and practices in the performance of contracts requiring access authorization(s).

(2) Criteria. The following criteria must also be satisfied for a board resolution to serve as the sole method accepted to negate or effectively reduce the risk of compromise arising from foreign ownership within the levels prescribed herein.

(a) Identified U.S. person(s) own a majority of the stock.

(b) A foreign person is not the single largest shareholder.

(3) Publication of the Resolution(s). The U.S. organization shall be required to distribute to its directors and its principal officers copies of such resolutions and report in its corporate records the completion of such distribution. In addition, the substance of the foregoing resolution(s) shall be brought to the attention of all personnel possessing or being processed for an access authorization.

(4) Verification. Compliance with the resolution(s) shall be verified during periodic surveys.

c. Security Control Agreement for Noncontrolling Foreign Minority Cases. When a foreign person(s) owns voting stock, directly or indirectly, and is permitted representation in the U.S. organization (that is, to hold a position as or appoint any of the U.S. organization's management and/or allowed to transfer any of its employees on any of its foreign-owned parent's or other foreign-owned affiliate's employees to the U.S. organization), the Security Control Agreement, as set forth in 11d(4), may be considered to negate or reduce the FOCI.

d. Controlling Foreign Majority Cases. A controlling foreign majority case is one in which foreign person(s) own a majority of the voting securities of the U.S. organization or, if less than 50 percent is foreign-owned, it can be reasonably determined that foreign person(s) or their representatives are in a position to effectively control or dominate the business management of the U.S. organization.

(1) Voting Trust Agreement. A voting trust agreement is an acceptable method to negate or reduce risks associated with a controlling foreign majority case. Under this arrangement, the following requirements must be met.

(a) Foreign stockholders must transfer legal title of foreign-owned stock to the trustees,

and the U.S. organization to be cleared must be organized, structured, and financed to operate as a viable business entity independent from the foreign stockholder(s).

(b) The Voting Trust Agreement must unequivocally provide for the exercise of all prerogatives of ownership by the trustees with complete freedom to act independently and without consultation with, interference by, or influence from foreign stockholders.

(c) There shall be at least three trustees, and all must become members of the U.S. organization's board of directors. In addition, the trustees must:

1 be U.S. citizens residing within the limits of the U.S. and capable of assuming full responsibility for voting the stock and exercising the management prerogatives relating thereto in such a way as to effectively insulate foreign stockholder(s) from the cleared U.S. organization;

2 be completely disinterested individuals with no prior involvement with either the cleared U.S. organization, its foreign-owned tier parent(s), and any of its foreign-owned affiliate(s);

3 be issued and be able to maintain an access authorization to the level of the facility clearance or safeguards and security activity;

4 be approved by the Office of Safeguards and Security when a vacancy occurs due to the resignation or removal of a trustee and a successor trustee is appointed by the remaining trustees;

5 prior to being accepted as trustees by the Office of Safeguards and Security, be advised by the Office of Safeguards and Security of the duties and their responsibilities on behalf of DOE to insulate the cleared U.S. organization from the foreign person(s), and indicate, in writing, their willingness to accept this responsibility.

(d) The voting trust agreement may, however, limit the authority of the trustees by requiring approval from the foreign stockholder(s) with respect to the following.

1 The sale or disposal of the cleared U.S. organization's assets or a substantial part thereof.

2 Pledges, mortgages, or other encumbrances on the capital stock they hold in trust.

3 Corporate mergers, consolidations, or reorganizations.

4 The dissolution of the cleared U.S. organization.

5 The filing of a bankruptcy petition.

(e) Trustees must assume full responsibility for the voting stock and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign stockholder(s), except for the approvals enumerated above, will be effectively insulated from the cleared U.S. organization and continue solely in the status of beneficiaries.

(f) The Certification and Visitation Approval Procedure Agreement of paragraph 11b(3) is required under this arrangement.

(2) Proxy Agreement. A proxy agreement is an acceptable method to negate or reduce risks associated with controlling foreign majority cases. Under this arrangement, the voting rights of stock owned by foreign persons are conveyed to proxy holders by an irrevocable proxy agreement. Legal title to the stock remains with the foreign persons. All other provisions of the voting trust agreement as they apply to trustees (see paragraph 11b(1)) and the terms of the agreement shall apply to the proxy holders. Conditions for consideration of use of a proxy agreement are the same as required for a voting trust agreement. Proxy agreements must be coordinated with General Counsel.

(3) Visitation Approval Procedure Agreement. In every case where a voting trust agreement or proxy agreement is employed to negate or reduce risks associated with foreign ownership, a visitation approval procedure agreement shall be executed between the cleared U.S. organization, the foreign persons, the Office of Safeguards and Security, and as appropriate, trustees, proxy holders, or other designated individuals. The visitation approval procedure agreement must identify who may visit, for what purposes, when advance approval is necessary, and the approval authority. The cleared U.S. organization shall submit individual requests to the approval authority for each visit. The visitation approval procedure agreement shall provide that, as a general rule, visits between foreign stockholder(s) and the cleared U.S. organization are not authorized; however, as an exception to the general rule, the approval authority may approve such visits in connection with regular day-to-day business operations pertaining strictly to purely commercial products or services and not pertaining to contracts requiring access authorization(s).

(4) Special Security Agreement and Security Control Agreements. The Special Security Agreement and the Security Control Agreements are substantially identical arrangements that impose substantial industrial security and export control measures within an institutionalized set of corporate practices and procedures; require active involvement of senior management and certain Board members in security matters (who must be cleared, U.S. citizens); provide for the establishment of a Government Security Committee to oversee classified and export control matters; and preserve the foreign stockholder's right to be represented on the Board with a direct voice in the business management of the company while denying unauthorized access to classified information.

(a) The Special Security Agreement may be considered to negate or reduce the FOCI for a U.S. organization effectively owned or controlled by a foreign person. However, access to proscribed information is permitted only with the written permission of the agency with classification or control jurisdiction over the proscribed information (e.g., NSA for COMSEC, DCI for SCI). A determination to disclose proscribed information to a company cleared under a Special Security Agreement requires that a favorable national interest determination be rendered prior to contract award. Additionally, DOE must have entered into a General Security Agreement with the foreign government involved (that is the country to which the foreign ownership stems).

(b) The Security Control Agreement may be considered to negate or reduce the FOCI for an organization not effectively owned or controlled by a foreign person. Limitations on access to classified information are not required under a Security Control Agreement.

12. REQUIREMENTS: ANNUAL REVIEWS AND COMPLIANCE.

a. Annual Review. Representatives of the Lead Responsible Office shall meet annually with senior management officials of organizations operating under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement to review the effectiveness of the pertinent security arrangement and to establish common

understanding of the operating requirements and how they will be implemented within the cleared organization.

b. Annual Certification.

(1) At the end of each year of operation, the trustees, proxy holders, or other principals as appropriate of those organizations operating under a DOE-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement shall submit to the Lead Responsible Office an annual implementation and compliance report. Failur ensure compliance with the terms of the appli in the organization's facility clearance being su FOCI.

(2) Each contractor holding a facility clearance shall certify annually to the Lead Responsible Office that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

(3) When the contractor is controlled by parent organizations that have been excluded, the contractor must also provide annually to the Lead Responsible Office written certification from an authorized official from each such excluded parent that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answers to the questions provided in its FOCI representations; (ii) no changes have occurred in the organizations's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

13. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager, telephone (301) 903-5217.

CHAPTER VII

INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. OBJECTIVES.

a. Programs and procedures shall be established to deter, detect, and ensure the prompt reporting of incidents of safeguards and security concern to DOE.

b. A systematic inquiry shall be conducted to review the circumstances surrounding an incident of safeguards and security concern to develop all pertinent information and to determine whether an infraction, criminal violation, or loss has occurred. Inquiries shall not be used as a means of holding in abeyance a decision to initiate a full-scale investigation.

2. APPLICABILITY. Incidents of safeguards and security concern are events that, at the time of occurrence, have yet to be determined to be a violation of law, but that are of such concern to the safeguards and security program as to warrant immediate review, inquiry, and subsequent assessment and reporting.

a. Safeguards and security representatives may conduct preliminary inquiries of incidents of Safeguards and Security concerns, however, they shall not investigate criminal violations except when DOE investigators are deputized agents of State or local law enforcement agencies. Such deputized agents shall consult with the Federal Bureau of Investigation when investigating criminal violations involving DOE and contractor activities, operations, or personnel.

b. When an inquiry establishes that an alleged or suspected violation of law involving a national security interest has occurred, the appropriate DOE Element shall refer the incident to the Federal Bureau of Investigation and/or the appropriate law enforcement agency.

c. When an inquiry establishes credible information that fraud, waste and/or abuse has occurred, which does not involve a national security interest has occurred, the Office of the Inspector General shall be notified for information and/or action.

d. When an inquiry establishes that a potential compromise or unauthorized disclosure of classified information has occurred, the applicable provisions of DOE O 471.2, INFORMATION SECURITY PROGRAM, shall be followed.

e. Employees with information regarding possible fraud, waste, abuse, or other forms of wrongdoing in the Department's programs or operations shall inform the Inspector General immediately upon obtaining such information.

3. REQUIREMENTS.

a. Safeguards and security directors shall ensure that inquiries are conducted to establish the circumstances surrounding as suspected or alleged criminal violation involving a national security interest or loss involving a national security interest. The authority to conduct such inquiries remains with the Head of the Field Element and, in the case of Headquarters, with the Office of Safeguards and Security.

(1) Inquiry officials (with previous inquiry experience) familiar with appropriate policies and procedures shall be appointed in writing by the Head of the DOE Element. The inquiry official is not authorized to detain individuals for interviews or obtain sworn statements; however, he/she may conduct consensual interviews and obtain signed statements. The inquiry official is responsible for maintaining records of inquiry (e.g., log of events, notes, recordings, statements).

(2) Whenever possible, the responsibility for an incident shall be fixed upon an individual rather than upon a position or office. When individual responsibility cannot be established, and the facts show that a responsible official allowed conditions to exist that led to an incident of safeguards and security concern, responsibility shall be fixed upon such responsible official. Infractions shall be issued in accordance with DOE O 471.2 for a violation of procedures after a determination has been made by the Department of Justice or appropriate authority not to prosecute the violation.

(3) An inquiry shall be instituted within 48 hours from the initial report of the alleged or suspected violation to the Office of Safeguards and Security and cognizant Secretarial Officer.

b. Loss, compromise, or unauthorized disclosure of classified information, and alleged or suspected violations of laws pertaining to safeguards and security shall be reported promptly through the appropriate DOE Element to the Office of Safeguards and Security, the Secretarial Officer, and when appropriate, the local Federal Bureau of Investigation office.

(1) The method and sequence for reporting safeguards and security incidents will depend upon the situation as well as the immediacy of action that may be required to mitigate the situation.

(2) Unclassified reports and notifications of safeguards and security incidents shall be made in accordance with DOE O 232.1 and DOE O 471.2. Reports that contain classified information shall contain all of the information required by DOE O 232.1, but shall not be

entered on the Occurrence Reporting and Processing System. Classified reports shall be sent by approved methods for transmitting classified information. Reporting intervals for incidents of safeguards and security concern must be in accordance with DOE O 232.1.

c. Federal Bureau of Investigation personnel shall be admitted to areas and afforded access to Restricted Data or other classified information as necessary for them to perform their duties. Such personnel shall be provided escort, as necessary, for safety reasons or to facilitate the investigative progress.

(1) When Federal Bureau of Investigation personnel are given access to classified information, they will be immediately advised of the classification and the category of the information. Appropriate document and data classification, marking information, and protection and control requirements shall be made available to them through local liaison channels.

(2) The availability of DOE standard security badges and advance notification arrangements shall be determined by agreement between the DOE and Federal Bureau of Investigation organizations involved. This authority does not extend to Sensitive Compartmented Information, which requires special access approval.

4. CONTACT. Comments and inquiries on this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER VIII

CONTROL OF CLASSIFIED VISITS PROGRAM

1. OBJECTIVES.

a. To ensure that only authorized persons with the appropriate access authorization and need-to-know receive access to classified information in connection with visits involving the release or exchange of classified information.

b. To limit foreign visitor access to classified information to that prescribed in approved Agreements for Cooperation and other bilateral security agreements.

2. APPLICABILITY. The requirements in this chapter apply to DOE personnel, covered contractors, and others who visit DOE facilities that entail access to Restricted Data and other classified information, and to DOE personnel and covered contractors that visit other specified Federal agencies.

3. REQUIREMENTS: CLASSIFIED VISIT PROCEDURES. Basic procedures for the control of all classified visits shall ensure the following:

a. Verification of the identity and need-to-know of the visitor.

b. The person's clearance or access authorization is at least equal to the classification of the information to which access is desired.

c. Observance of limitations on access to classified information or facilities. Access to certain programs or information is handled in accordance with the following:

(1) Weapons Production Programs. For access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, requests shall be referred to the Assistant Secretary for Defense Programs.

(2) Uranium Enrichment. For access to uranium enrichment plants or facilities engaged in

uranium enrichment technology development, including advanced isotope separation technology, the request shall be referred to the Office of Uranium Programs.

(3) Naval Nuclear Propulsion Information. When access is desired to Naval Nuclear Propulsion Information, the request shall be referred to the Office of Naval Reactors.

d. Timely notification of visits.

e. Prompt transmittal of "Request for Visit or Access Approval" (DOE F 5631.20), when applicable. (This form is no longer required for DOE and DOE contractor employees who visit DOE facilities. These employees may use their DOE picture identification badge as evidence of a DOE access authorization. However, DOE F 5631.20 is still required for programmatic approval for sigma access and for employees of other Federal agencies who visit DOE facilities.)

f. Timely notification to those concerned for approval of access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by Headquarters Elements.

g. Use of continuing visitor access approval as necessary for individuals who visit DOE facilities frequently. This approval cannot exceed a period of 1 year, but the approval may be renewed annually, if necessary.

h. Operational approval of visits.

i. Maintenance of records of all classified visits by non-DOE personnel and foreign nationals.

j. Referral to the Director of Public and Consumer Affairs of any nonroutine, written, or visual material proposed for public release resulting from visits.

k. The Director of Safeguards and Security shall maintain liaison with the Department of Defense, National Aeronautics and Space Administration, and other Federal agencies in order to:

(1) ensure that DOE is notified of changes in those positions whose occupants are authorized to initiate access requests; and

(2) provide assistance in identifying DOE Elements and Federal offices to which specific requests shall be directed.

4. REQUIREMENTS: CLASSIFIED VISITS BY DOE EMPLOYEES, CONTRACTORS AND SUBCONTRACTORS.

a. The visitor is responsible for making administrative arrangements and obtaining approval from the Departmental Element, as appropriate. (The authority granting such approval is responsible for informing the office to be visited.)

b. Contractors or subcontractors with mutual program interests may be authorized, subject to the limitations in subparagraph c below, to arrange for visits without obtaining DOE approval if such authorization will be advantageous to the DOE.

c. The following procedures are required when access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, inertial confinement fusion data, atomic vapor laser isotope separation technology, uranium enrichment technology, or specific facilities designated by Headquarters Elements having program direction is required.

(1) Approval of the access during visits under the auspices of a Headquarters Element shall be obtained from the Headquarters Element exercising jurisdiction over the facility or office to be visited.

(2) Approval of this access during visits under the auspices of Field Elements shall be obtained from the responsible Field Element for field visits and for visits to Headquarters from the organization being visited.

5. REQUIREMENTS: VISITS TO DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION FACILITIES. Both agencies accept DOE access authorizations for Restricted Data and other classified information under their jurisdiction on the same basis as DOE, provided access authorization and "need-to-know" are properly certified.

a. DOE Top Secret approvals shall be specifically certified in the event access to Top Secret information is required.

b. A DOE F 5631.20, "Request for Visit or Access Approval" shall be forwarded directly to the military or civilian official with jurisdiction over the information to which access is desired.

c. Any exchange of Restricted Data occurring during the course of the visit shall be accomplished as stated in paragraph 7 below.

6. REQUIREMENTS: RESTRICTED DATA VISITS BY NUCLEAR REGULATORY COMMISSION EMPLOYEES.

a. Visits to DOE facilities by Nuclear Regulatory Commission employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology, or entry into a DOE classified weapon or production facility shall:

(1) be arranged through the respective Headquarters Element that will coordinate the visits;

(2) if to classified weapon or production facilities, have prior approval of the Assistant Secretary for Defense Programs;

(3) have DOE F 5631.20 or the Nuclear Regulatory Commission equivalent with necessary clearances certified by the Director of Security, Nuclear Regulatory Commission.

b. Visits involving access to other Restricted Data not requiring prior approval from the appropriate Headquarters official exercising jurisdiction over the facility or office to be visited may be arranged
directly by Nuclear Regulatory Commission with the cognizant DOE Element, provided this procedur does not conflict with the existing visitor control procedures of the division or office having program responsibility. A DOE F 5631.20 or Nuclear Regulatory Commission equivalent is required.

c. The Nuclear Regulatory Commission identification badge shall not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

7. REQUIREMENTS: RESTRICTED DATA VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES.

a. Access to Restricted Data is contingent upon submission of a DOE F 5631.20, National Aeronautics and Space Administration Form-405, "Request for Access Approval," or a memorandum or electronic message signed by or in the name of the certifying official. The request shall be forwarded for approval or other action to the DOE official with jurisdiction over the information to which access is desired.

b. The request for access shall include the following:

(1) Name(s) of person(s) and organization represented (if not Armed Forces, relationship to the Department of Defense or National Aeronautics and Space Administration).

(2) Facility and information to which access is desired. Access to critical nuclear weapon design information must be specified when it is required.

(3) The security clearance or access authorization status of each person, including clearance date.

(4) Purpose of visit and certification that the person needs the access in the performance of duty.

(5) Anticipated date of visit and names of persons to be visited, as appropriate. (If a conference is involved, the date, place, and sponsor of the conference shall be specified.)

(6) Citizenship, date of birth, and social security number.

(7) For requests from National Aeronautics and Space Administration, a certification that the matter to which access is desired relates to "aeronautical and space activities."

c. The approving official must possess or have been delegated the authority to approve such access.

d. Control of access by members of the Armed Services or by Department of Defense or National Aeronautics and Space Administration personnel or contractors to Restricted Data in the custody of another Federal agency is the responsibility of the appropriate official or his/her designee named in Chapter VIII, Attachment VIII-1.

e. Headquarters Elements shall retain for 3 years a copy of each visit request they have approved. Separate records shall be maintained for approvals of access under emergency conditions.

8. REQUIREMENTS: OTHER CLASSIFIED VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES .

a. Requests for such visits to DOE and contractor and subcontractor facilities are approved by Heads of Field Elements or, in the case of Headquarters Elements, by the head of the element concerned after ensuring that such visitor possesses appropriate military or National Aeronautics and Space Administration security clearance and requires the information in the performance of his/her duties.

b. Certification of security clearance may be made by memorandum, electronic message, DOE F 5631.20, or National Aeronautics and Space Administration Form 405.

9. REQUIREMENTS: CLASSIFIED VISITS BY EMPLOYEES OF OTHER FEDERAL AGENCIES.

a. Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than the Department of Defense, National Aeronautics and Space Administration, or Nuclear Regulatory Commission are approved by the Field Elements or, for Headquarters, by the organization concerned.

b. Restricted Data may not be exchanged with persons in this category unless they possess appropriate DOE access authorization.

c. Classified information other than Restricted Data may be exchanged with such individuals if

they possess Q or L access authorizations or security clearances under the provisions of Executive Order 10450, "Security Requirements for Government Employment," and require the information in the performance of their duties.

10. REQUIREMENTS: CONGRESSIONAL AND STATE CLASSIFIED VISITS.

a. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by Governors or their staffs may be approved by Heads of DOE Elements provided the following are established.

(1) The visitors' identities.

(2) Access authorization or security clearance.

(3) "Need-to-know."

b. The Assistant Secretary for Congressional and Intergovernmental Affairs shall be advised of requests and action taken on the requests for such visits.

11. REQUIREMENTS: EMERGENCY VISITS TO CLASSIFIED AREAS AND FACILITIES.

a. In an emergency, requests for visit approval may be made by telephone or electronic message.

b. Telephonic requests must be confirmed by memorandum or electronic message.

12. REQUIREMENTS: CLASSIFIED VISITS BY FOREIGN NATIONALS TO DOE FACILITIES. Classified visits by foreign nationals sponsored by a foreign government shall be arranged as follows.

a. If the visit is in connection with the military application of atomic energy under sections 144b and c(1) and 91c(1) or (4) of the Atomic Energy Act of 1954, as amended, the Assistant Secretary for Defense Programs shall make all arrangements for the visit, including appropriate approvals and security assurances.

b. If the visit is to the Office of Declassification in connection with the information classification program under DOE 5650.2B, the Director of Declassification shall make arrangements for the visit, including appropriate approvals and security assurances.

c. If the visit is not in connection with programs covered in the above paragraphs, the Deputy Assistant Secretary for International Energy Policy shall arrange for the visit in concert with the appropriate Headquarters staff other than those listed above, and shall coordinate with the Director of Safeguards and Security for the necessary security assurances.

d. If the visit will include discussions on naval nuclear propulsion matters, the Director of Naval Reactors shall be informed and review the visit for approval. The Director of Safeguards and Security may be requested to obtain the necessary security assurances.

e. Security assurances received under the above paragraphs shall be retained for 5 years.

13. CONTACT. Comments and inquiries on this chapter may be directed to the Personnel Security Policy Program Manager at (301) 903-3200.

ACCESS TO RESTRICTED DATA
IN POSSESSION OF OTHER FEDERAL AGENCIES

The following Federal officials are authorized to permit their Federal and contractor employees possessing DOE access authorizations to grant access to Restricted Data in their possession to members of the Armed Forces and Department of Defense and National Aeronautics and Space

Administration employees and their contractors, in accordance with section 143 of the Atomic Energy Act of 1954, as amended, and subsection 304(b) of the National Aeronautics and Space Act of 1958.

The Assistant to the President
Director, Office of Management and Budget
Executive Secretary, National Security Council
Director, Central Intelligence Agency
Director, Federal Emergency Management Agency

Secretary of State
Secretary of the Treasury
Attorney General of the United States
Secretary of the Interior
Secretary of Agriculture
Secretary of Commerce
Secretary of Labor
Secretary of Health and Human Services
Secretary of Transportation
Secretary of Education

Chairman, Federal Communications Commission
Administrator, Agency for International Development
President, National Academy of Sciences and National Research Council

Director, National Science Foundation
Chairman, Tennessee Valley Authority
Director, United States Information Agency

Comptroller General of the United States

CHAPTER IX

SURVEY PROGRAM

1. POLICY/OBJECTIVES. To ensure proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contract employees, the public, or the environment are afforded safeguards and security activities. The adequacy of safeguards and security measures shall be validated through various means, such as:

   a. surveys conducted by the DOE Surveying Office prior to initiation of safeguards and security activities and periodically thereafter;

   b. periodic facility self-assessments;

   c. program reviews by Facility Survey Operations Managers and other appropriate Departmental Elements; and

   d. inspections and assessments by the Deputy Assistant Secretary for Independent Oversight and Appraisals.

2. APPLICABILITY. The Survey Program applies to all facilities that are eligible to have access to, use, store, or transmit nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat and/or classified information, that require access authorizations, or that possess over $5,000,000 of DOE property, exclusive of facilities and land values.

3. TYPES OF SURVEYS.

a. Initial. A comprehensive survey conducted at the facility before granting approval.

b. Periodic. A comprehensive survey conducted at the facility at scheduled intervals.

c. Special. A survey conducted at the facility for a specific, limited purpose such as for a technical security reason (i.e., Technical Surveillance Countermeasures surveys or services), a detailed review of a problem area, an unannounced survey, shipment of nuclear materials or classified material, or change in the contractor operating a government-owned facility. Shipments between sites by rail, truck, air, or ship are subject to survey unless the shipment is made via commercial carrier licensed by the Nuclear Regulatory Commission.

d. Termination. A survey of a facility conducted when all safeguards and security activities have been removed, access authorizations terminated, and close out of required records accomplished, to ensure proper disposition of classified matter and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat. Termination of facility clearances for facilities possessing Top Secret matter or special nuclear material require an onsite termination survey. For other facilities, termination may be by onsite survey or correspondence.

4. SCOPE OF SURVEYS.

a. Compliance. The compliance segment of a facility survey reflects the status of a facility's safeguards and security system as measured against implementation of applicable Federal statutes, regulations, policy, and approved safeguards and security plans.

b. Performance. The performance segment of a facility survey reflects the degree to which the elements of the safeguards and security system meet protection objectives based upon operational testing of the system.

c. Comprehensive. Comprehensive surveys cover the protection afforded safeguards and security activities and interests within a facility, including an evaluation of the adequacy and effectiveness of safeguards and security programs and a thorough examination of policies and procedures to ensure compliance and performance. All applicable topical areas, identified on DOE F 5634.1, "Safeguards and Security Survey Report," must be surveyed, except as identified in paragraph 5c.

d. Other. The scope of special and termination surveys shall be determined by coordination between the Lead Responsible Office and the Surveying Office. The basis for scope determinations shall be established by the nature or status of operations at the facility, activity, or element being surveyed. These surveys need not cover all topical areas identified on DOE F 5634.1.

5. REQUIREMENTS: FREQUENCY OF SURVEYS.

a. Initial surveys are not required for non-possessing facilities. Termination surveys of non-processing facilities are not required; however, a review shall be conducted and documented to verify that access authorizations have been terminated.

b. Periodic surveys shall be conducted in accordance with the following schedule.

(1) Facilities possessing classified matter or Category III or greater nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat shall be surveyed once every 12 months.

(2) Facilities possessing property protection interests shall be surveyed once every 24 months.

(3) Facilities that do not possess classified matter but do issue access authorizations to employees to satisfy contractual obligations shall be reviewed at least once every 5 years and not necessarily through an on-site survey. The review shall validate access authorizations and FOCI information.

(4) For facilities containing only Category IV nuclear materials as defined in DOE 5633.3B, the materials control and accountability topical area shall be surveyed at least once every 24 months. If the total inventory consists entirely of source material, less than 10 tons of heavy water, less than 350 grams of special nuclear materials, or any combination of these, a survey of the materials control and accountability topical area is not required.

c. The results of prior surveys may affect the scheduling frequency. An extended survey schedule (up to 24 months) may be implemented by the Surveying Office after consultation with the Lead Responsible Office if the facility has:

(1) a facility security staff trained and knowledgeable in safeguards and security requirements, as evidenced by past performance in surveys;

(2) an ongoing self-assessment program covering all survey topics and sub-topics with the results reported to the Lead Responsible Office;

(3) no significant deficiencies resulting from self-assessments or surveys (including no less than a satisfactory rating at the topic levels); and

(4) an approved site safeguards and security plan.

Schedules for facilities with Category I special nuclear materials may be extended if all conditions above have been met.

d. Reviews, including inspections, conducted by Departmental Elements other than the Surveying Office or other Government oversight offices, may be used to meet survey requirements. Topics and subtopics on DOE F 5634.1 that are not addressed during reviews must be surveyed by the Surveying Office. When using reviews to meet the requirements of the survey, the following guidelines shall be followed.

(1) The review must have been conducted within the surveyed period.

(2) Portions of the review used must be attached to the survey.

(3) Topics and subtopics not covered by the review must be surveyed.

(4) If ratings were not assigned, ratings must be assigned for those reviews that are used. After the review is conducted, the Surveying Office shall analyze the impact of any deficiencies and assign ratings.

e. Special surveys shall be conducted as determined by the Lead Responsible Office.6. REQUIRE

a. Survey Responsibility. The Lead Responsible Office must ensure surveys are conducted. The responsibility for conducting surveys may be transferred to another Surveying Office and documented on DOE F 5634.3. Secretarial Officers shall function as the Surveying Office for those offices identified in Chapter I, paragraph 7, by ensuring that periodic surveys are completed. Lead Responsible Offices for facilities that ship nuclear materials are responsible for conducting shipment surveys.

b. Survey Team Composition. Survey teams are composed of inspectors and support service personnel. All survey teams shall be led by a Federal employee. Team personnel for surveys shall possess qualifications, experience, and training sufficient to accomplish effective and

thorough surveys. New inspectors must attend basic survey training.

c. Planning. The survey process and requirements shall be documented in locally approved survey guidelines. Surveying Offices shall coordinate planning with the Lead Responsible Office and other organizations with registered safeguards and security activities.

d. Coordination of Surveys.

(1) Safeguards and security surveys should be conducted in an integrated manner. If performed separately, the Surveying Office shall document the responsibility for each survey activity and coordinate submission of a single survey report that includes a composite facility rating.

(2) Survey field activities conducted separately must be completed within 30 working days of each other, except as identified in paragraph 3c above.

e. Validation. To ensure accuracy, survey results shall be validated by discussion, observations, or exercises during the survey period.

f. Closeout. A final closeout briefing shall be conducted with the surveyed organization to present, at a minimum, the following items.

(1) Each finding.

(2) Topical ratings and the overall composite rating.

(3) Corrective action reporting requirements.

7. REQUIREMENTS: SURVEY REPORTS.

a. Report Content. Reports shall describe the conduct, results, and evaluation of the safeguards and security program and shall include the following minimum requirements.

(1) A completed DOE F 5634.1.

(2) An executive summary containing:

(a) a statement reflecting survey scope, period of coverage, and survey methodologies used;

(b) a description of the facility, function, and scope of operations;

(c) a discussion of major points that had, or might have, a significant effect on the facility's safeguards and security program, including strengths, weaknesses, and the correlation of results from the survey; and

(d) the overall composite facility rating with supporting rationale.

(3) The report, which must include:

(a) a copy of the current DOE F 5634.3;

(b) identification of each active DOE F 5634.2 (or DD 254);

(c) a description of the facility's safeguards and security program by topical area as identified on the DOE F 5634.1;

(d) the methodology used to evaluate the facility;

(e) a description of the function and scope of operations and the protective measures employed (descriptions in safeguards and security plans may be referenced when no changes have occurred);

(f) identification of all new findings;

(g) the status of corrective actions for all open findings and status of all open and closed findings from the previous survey;

(h) concluding analysis of each topical area; and

(i) a justification and rationale of the factors responsible for the composite facility rating.

b. Termination Survey Reports. Termination survey reports shall include the following minimum information/reported action.

(1) Verification of non-possession of classified matter or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat.

(2) Verification that personnel access authorizations no longer needed have been canceled and validation that termination statements have been completed by affected employees.

(3) Verification of deletion of all safeguards and security activities.

(4) Termination of facility clearance.

c. Distribution. Within 60 working days after final closeout of the survey, the Surveying Office shall distribute the final survey report to all Departmental Elements with a registered activity and to all appropriate Headquarters Elements. For Departmental Elements or other government agencies with limited safeguards and security activities, survey results may be transmitted by memorandum.

8. REQUIREMENTS: RATING SYSTEM. The composite facility rating shall be based on the effectiveness and adequacy of the safeguards and security at a facility and reflect a balance of performance and compliance as determined by the Surveying Office. Ratings are not assigned for termination surveys.

a. Types of Ratings.

(1) Satisfactory. The safeguards and security element being evaluated meets protection objectives or provides plausible assurance that protection needs are being met.

(2) Marginal. The safeguards and security element being evaluated only partially meets protection objectives or provides questionable assurance that protection needs are being met.

(3) Unsatisfactory. The safeguards and security element being evaluated does not meet protection objectives or does not provide adequate assurance that protection needs are being met.

b. Basis for Ratings.

(1) Ratings are based on conditions existing at the end of survey activities. Ratings shall not be based upon future or planned corrective actions.

(2) If corrective actions are taken before assignment of the survey rating at closeout, the final rating shall reflect validated corrective actions only.

(3) Marginal or unsatisfactory ratings in any topical area shall be based on validated weaknesses in the safeguards and security system or deficiencies in performance in an operational area. Failure to comply with procedural documentation requirements, of and by itself, shall not normally be the basis for a reduction in a rating.

c. Use of Marginal Ratings. A facility composite rating or topical area rating shall not be marginal for consecutive survey periods unless one of the following conditions apply.

(1) The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.

(2) The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a major line-item construction project or upgrade program. In that case, acceptable interim measures must have been implemented and physically validated pending completion of the project. These interim measures and milestones for construction completion shall be documented in the survey report.

(3) If neither of the above conditions apply, an unsatisfactory rating shall be assigned.

d. Survey Report. Ratings shall be based on the impact of deficiencies. All ratings must be stated and justified in the survey report.

9. REPORTING REQUIREMENTS: MARGINAL AND UNSATISFACTORY COMPOSITE RATINGS. Reporting requirements identified below are initiated by the final close-out briefing.

a. Marginal. Within 15 working days following a survey closeout that results in an overall composite rating of marginal, the Lead Responsible Office shall notify the Office of Safeguards and Security, and the applicable Departmental Elements. Notification shall contain the following.

(1) Identification of the facility (including both the facility code and reporting identification symbol - if applicable).

(2) A list of findings describing the deficiencies.

(3) A description of corrective actions taken to date or planned with associated milestones.

(4) A justification statement addressing the overall composite rating and status of the safeguards and security program at the facility.

(5) A statement identifying risks or vulnerabilities.

(6) A statement acknowledging physical validation of adequacy of interim corrective actions taken to date.

(7) A statement outlining steps that shall lead to the upgrading of the overall composite rating to satisfactory.

If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall notify the Lead Responsible Office of results and rating(s) within 72 hours of survey closeout. The Lead Responsible Office shall then take corrective and notification actions outlined in this chapter or authorize the Surveying Office to take those actions.

If the Surveying Office is unable to contact the Lead Responsible Office and a serious threat

exists or is imminent, the Surveying Office shall take action to protect safeguards and security activities until the Lead Responsible Office can be notified. Subsequent action shall be taken on the basis of agreement between the two organizations and shall be fully documented in the survey report.

b. Unsatisfactory. When a survey results in an overall composite rating of unsatisfactory, the Operations Office Manager of the Lead Responsible Office shall coordinate with Secretarial Officers and other Heads of Operations Offices within 24 hours to:

(1) take action to suspend the activity and/or the facility clearance pending remedial action or

(2) provide the rationale for continuing this critical operation to the Office of Security Affairs, the Office of Safeguards and Security, Secretarial Officers, and as directed, applicable Operations Offices. In addition to providing the rationale, the Lead Responsible Office must identify those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall notify the Lead Responsible Office of the results and rating(s) within 8 hours of survey closeout.

If the Surveying Office is unable to contact the Lead Responsible Office, action shall be taken to protect safeguards and security activities until the Lead Responsible Office can be notified. Subsequent action will be taken on the basis of agreement between the two organizations and shall be fully documented in the survey report.

c. Change of Rating. When the Lead Responsible Office determines that the composite survey rating shall be upgraded, the Lead Responsible Office shall then notify the Office of Safeguards and Security and the appropriate Secretarial Officer.10. REQUIREMENTS: CORRECTIVE ACTIOI

a. When a survey contains findings, the surveyed organization shall submit a response identifying corrective action(s) for each finding to the Responsible and Surveying Offices no later than 30 working days after formal receipt of findings. The corrective action(s) should be based on documented root cause analysis, risk assessment, and cost-benefit analysis.

b. When a survey indicates a composite rating of satisfactory but contains findings requiring corrective action, the Lead Responsible Office shall enter the findings and status of corrective actions in the Safeguards and Security Information Management System and quarterly provide electronic status notification to the Office of Safeguards and Security, the appropriate Secretarial Officers, and the Surveying Office (if appropriate).

c. When a survey has a composite rating of marginal, the Lead Responsible Office shall notify the Director, Office of Safeguards and Security, the Surveying Office (if appropriate), and the applicable Operations Office and Secretarial Officer(s) within 15 working days after completion of the survey.

(1) The notification must address interim corrective actions taken, or to be taken, to correct identified risks or vulnerabilities.

(2) If interim corrective actions are instituted, the Surveying Office shall physically verify them for adequacy.

(3) If the Surveying Office is not the same as the Lead Responsible Office, the Surveying Office shall promptly notify the Lead Responsible Office of the rating. The Lead Responsible Office shall then take appropriate corrective and notification actions outlined above or authorize the Surveying Office to take those actions.

(4) If the Surveying Office is unable to contact the Lead Responsible Office and a serious threat exists or is imminent, the Surveying Office shall take action to protect the safeguards and security interest(s) until the Lead Responsible Office is notified. Subsequent action shall be taken on the basis of agreement between the two organizations.

d. When a survey has a composite rating of unsatisfactory, and the rating indicates a significant vulnerability, such as **unacceptable risk** of special nuclear material theft, radiological sabotag toxicological sabotage, or industrial sabotage or espionage, the Operations Office Manager shall coordinate with the cognizant Program Secretarial Officer 24 hours to:

(1) take action to shut down/suspend operation of the facility or activity, pending remedial action or

(2) apprise the cognizant Secretarial Officer and the Office of Safeguards and Security of the rationale for continuing this critical operation and identify those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

For all other unsatisfactory ratings, the Operations Office Manager of the Lead Responsible Office shall notify the cognizant Secretarial Officer and the Office of Safeguards and Security within 15 working days of interim corrective actions taken, or to be taken, to correct identified risks or vulnerabilities.

e. When either a marginal or unsatisfactory composite rating is assigned, the Lead Responsible Office shall provide to the Office of Safeguards and Security and the applicable Operations Office and Secretarial Officer(s) quarterly status reports on completed or planned corrective actions (with associated milestone dates) until all have been completed. When the Lead Responsible Office determines that the composite survey rating should be upgraded to satisfactory, the Surveying Office shall physically verify the completion and adequacy of corrective actions. The Lead Responsible Office shall then notify the Director, Office of Safeguards and Security, and the Cognizant Secretarial Officer(s) that the rating should be upgraded.

f. A finding associated with a significant vulnerability shall not be considered closed until associated corrective action has been completed and the Office of Safeguards and Security and the Secretarial Officer(s) are notified. A commitment by the facility to institute corrective action does not constitute completion of that corrective action.

11. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CHAPTER X

SELF-ASSESSMENT PROGRAM

1. OBJECTIVE. A safeguards and security self-assessment program shall be implemented to ensure internal monitoring of compliance and performance with safeguards and security requirements.

2. APPLICABILITY. This program applies to Departmental and contractor facilities for which a DOE F 5634.3 is recorded. The level of detail of the self-assessment may be specified by the Lead Responsible Office.

3. REQUIREMENTS.

a. Self-assessment programs shall be conducted and documented for all approved facilities. The self-assessment program shall:

(1) include reviews of all applicable DOE F 5634.1 topical and subtopical areas of the

facility's safeguards and security program/system;

(2) be conducted between the periodic surveys conducted by the Surveying Office; and

(3) be conducted using personnel knowledgeable of the programmatic or topical area.

b. Self-assessment reports shall:

(1) address reviewed topical areas;

(2) be used as organizational management tools/aids in determining the status of safeguards and security performance and compliance with applicable safeguards and security Order requirements;

(3) be available for review by the Surveying Office during surveys; and

(4) list findings resulting from self-assessment activities.

c. Findings resulting from self-assessments shall be processed as follows.

(1) Reviewed during the surveys by the Surveying Office.

(2) Addressed by facility/organization management through a documented corrective action plan.

(3) Reviewed and the status of findings tracked until closed.

(4) Reported to the Lead Responsible Office if:

(a) a vulnerability to national security, classified information, nuclear materials, or Departmental property results, or may result, in a significant anomaly that could have significant programmatic impact or embarrass the Department; or

(b) the self-assessment is used to extend the Surveying Office's periodic survey frequency.

(5) Documented in survey reports when deficiencies still exist and have not been adequately addressed.

4. CONTACT. Comments and inquiries regarding this chapter may be directed to the Technical and Operations Security Program Manager at (301) 903-5217.

CONTRACTOR REQUIREMENTS DOCUMENT

CONTRACTOR SAFEGUARDS AND SECURITY PROGRAM REQUIREMENTS

The intent of the following requirements is that Department of Energy (DOE) contractors and their employees will adhere to the same standards for protection of materials, information, and other property of interest to the Department's Safeguards and Security Program against loss, theft, sabotag or other hostile acts, as those required of DOE Elements and their personnel.

1. RISK MANAGEMENT. The acceptance of some level of risk is inherent in any activity. The nature of the threat, the vulnerability of the potential target, and the potential consequences of

an adversarial act shall be considered in determining the appropriate level of protection against risk. Accordingly, safeguards and security programs shall be based on vulnerability/risk analyses designed to provide graded protection in accordance with the asset's importance. Risk associated with safeguards and security vulnerabilities should be reduced even where not mandated by specific requirements, when such reduction is consistent with DOE's mission and when supported by appropriate cost/benefit analyses.

2. SITE-SPECIFIC PROGRAMS. Safeguards and security programs shall be tailored to address site-specific characteristics. Site-specific protection programs shall be documented. Risks to be accepted by the Department shall be identified and documented by vulnerability/risk analyses.

3. THREAT POLICY. The Design Basis Threat Policy, issued by the Director of Security Affairs, shall be used in the design and implementation of protection programs.

4. COMPARABILITY. Safeguards and security programs shall be comparable in effectiveness to other Federally regulated programs with similar interests, when such levels are consistent with DOE protective needs and national security interests.

5. STANDARDIZATION.

   a. Safeguards and security equipment and systems shall be selected on the basis of cost savings or other benefit to DOE such as worker safety, compliance with life safety codes, enhancing mission capability, and facilitating contingency efforts.

   b. New facility designs shall incorporate the use of standardized safeguards and security equipment and systems, where possible without compromising design flexibility or adherence to performance criteria.

6. DEVIATIONS. Alternate or equivalent means of providing adequate safeguards and security may be proposed to meet a specific Safeguards and Security Program requirement, when justified. When submitting such a request, the contractor shall specify the reasons why it is impractical or unreasonable to comply with a requirement. The following procedures and approval levels shall apply to all such deviations from requirements.

   a. Variances are approved conditions that technically vary from a Safeguards and Security Program requirement, but afford equivalent levels of protection without compensatory measures.

      (1) Contractors shall submit requests for variances through established channels.

      (2) Variances may be approved for an indefinite period.

      (3) Variances shall be documented in the appropriate safeguards and security planning documents.

   b. Waivers are approved nonstandard conditions that deviate from a Safeguards and Security Program requirement that, if uncompensated, would create a potential or real safeguards and security vulnerability. Waivers therefore require implementation of compensatory measures for the period of the waiver (e.g., expenditure of additional resources to implement enhanced protection measures).

      (1) Contractors shall submit requests for waivers through established channels.

      (2) A waiver shall be for a period not to exceed 2 years.

   c. Exceptions are approved deviations from a Safeguards and Security Program

requirement that create a safeguards and security vulnerability. Exceptions shall be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk. Contractors shall submit requests for exceptions through established channels.

(1) Exceptions shall be for a period not to exceed 3 years.

(2) The need for an exception shall be validated annually.

(3) Exceptions shall be included in Site Profiles, which form the basis for DOE's Annual Report to the President on the Status of Safeguards and Security.

d. Documentation. Specific information to be included to document each deviation is provided in Attachment 2. Approved deviations shall be documented in safeguards and security documents. A deviation request approved out of cycle with the safeguards and security plan formulation and approval process shall be documented as an attachment to the applicable safeguards and security plan.

e. Vulnerability Analyses and Performance Testing. Compensatory measures implemented and used as the basis for an exception request shall be subject to formal vulnerability assessments and must be performance tested and validated by the cognizant Field Element. The results of the vulnerability assessment(s) and performance tests shall be documented in the Site Safeguards and Security Plan. Performance testing and documentation, as necessary, may also be required for locally approved variances and waivers.

f. Validations. Cognizant Heads of Program Offices and Office of Safeguards and Security representatives may perform on-site reviews, assessments, and validation visits to ascertain the nature and impact of deviation requests.

g. Corrective Actions. Contractors shall monitor corrective actions, establish schedules, and ensure that funding is effectively managed to address safeguards and security interests and monitor compliance with schedules.

TABLE OF CONTENTS

Page

CHAPTER I - SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. Applicability. I-1
2. Planning Requirements. I-1
3. Planning Documents I-2

CHAPTER II - SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. Applicability. II-1
2. Program Requirements II-1

CHAPTER III - PERFORMANCE ASSURANCE PROGRAM

1. Applicability. III-1
2. Program Requirements III-1
3. Documentation Requirements III-3

CHAPTER IV - SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. Applicability. IV-1
2. Requirements: Summary of Safeguards and Security

Awareness Program. IV-1
3. Documentation Requirements IV-3

CHAPTER V - FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. Applicability. V-1
2. Requirements: General. V-1
3. Requirements: Facility Clearances V-2
4. Requirements: Facility Data and Approval Record . . . V-3
5. Requirements: Contract Security Classification SpecificationV-3

CHAPTER VI - FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. Applicability. VI-1
2. Requirements VI-1
3. Requirements: Reporting Significant Changes VI-2
4. Requirement: Methods to Negate or Reduce Unacceptable FOCIVI-2
5. Requirements: Annual Certification. VI-3

CHAPTER VII - INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. Applicability VII-1
2. Requirements. VII-2

CHAPTER VIII - CONTROL OF CLASSIFIED VISITS PROGRAM

1. Applicability VIII-1
2. Requirements: Classified Visit Procedures. VIII-1
3. Requirements: Classified Visits by DOE Employees, Contractors and SubcontractorsVIII-2
4. Requirements: Visits to Department of Defense and National Aeronautics and Space Administration Facilities VIII-2
5. Requirements: Restricted Data Visits by Nuclear Regulatory Commission and EmployeesVIII-2
6. Requirements: Restricted Data Visits by Department of Defense and National Aeronautics and Space Administration Employees. VIII-3
7. Requirements: Other Classified Visits by Department of Defense and National Aeronautics and Space Administration Employees. VIII-5
8. Requirements: Classified Visits by Employees of Other Federal Agencies. VIII-5
9. Requirements: Congressional and State Classified VisitsVIII-5
10. Requirements: Emergency Visits to Classified Areas and Facilities. VIII-6
11. Requirements: Classified Visits by Foreign Nationals to DOE FacilitiesVIII-6

CHAPTER IX - SURVEY PROGRAM

1. Applicability IX-1
2. Requirements: Corrective Actions IX-2

CHAPTER X - SELF-ASSESSMENT PROGRAM

1. Applicability X-1
2. Requirements. X-1

CHAPTER I

SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. APPLICABILITY. This chapter applies to contractors that have responsibilities for administering

and/or protecting the following sites and facilities.

a. Those that have Category I quantities of special nuclear materials, or those that have Category II quantities within the same Protected Area that roll-up to a Category I quantity.

b. Those that have a radiological/toxicological sabotage threat that would cause an unacceptable impact on the national security, the health and safety of employees, the public, or the environment.

c. Those that have an industrial sabotage threat that would cause an unacceptable impact to those DOE programs supporting national defense and security.

d. Those facilities engaged in intra-site transfer of special nuclear material.

e. Those facilities possessing classified matter.

f. Those facilities engaged in the protection of government property.

g. Other facilities/sites that Heads of DOE Elements deem appropriate based on vulnerability analyses.

2. PLANNING REQUIREMENTS. The following topics shall be essential elements for planning Safeguards and Security programs.

a. Site-Specific Characteristics. Protection programs shall be tailored to address specific site characteristics and requirements, current technology, ongoing programs, operational needs, and to achieve acceptable protection levels that cost-effectively reduce inherent risks.

b. Threat. The "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall be used in conjunction with local threat guidance and vulnerability assessments for protection and control program planning.

c. Protection Strategy

(1) A denial strategy shall be used for protection of Category IA special nuclear material and radiological sabotage targets where unauthorized access represents **unacceptable risk**. Programs shall be designed to prevent unauthorized control (i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials to assemble an improvised nuclear device onsite).

(2) A containment strategy shall be used to prevent the unauthorized removal of Category II or greater special nuclear material.

(3) Should denial or containment fail, a recapture/recovery or pursuit strategy shall be employed.

(4) Programs shall be designed to mitigate the consequences of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

(5) Strategies for protection and control of classified matter shall incorporate the applicable requirements established in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94; DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM, of 7-15-94; and DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL. Emphasis shall be placed on security systems capable of detecting or

deterring unauthorized disclosure, modification, or loss of classified and sensitive unclassified information and its unauthorized removal from a site or facility.

(6) Strategies for protection of government property not covered in subparagraphs (1) and (2) above shall reflect a graded approach.

(7) Security countermeasures to address bombings shall consider a range of activities from hand-carried, or mailed, to vehicle-transported devices.

d. Graded Protection Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

3. PLANNING DOCUMENTS

a. Site Safeguards and Security Plan This plan is the master planning document that shall be prepared for sites with facilities described in paragraphs 2a, 2b, 2c, and 2d. The plan shall depict the existing condition of safeguards and security sitewide and by facility, and establish improvement priorities, and resource requirements for the necessary improvements. The plan shall contain information that describes:

(1) protection strategies;

(2) site/facility safeguards and security programs in place or planned;

(3) plans and procedures designed to implement, manage, and maintain safeguards and security programs;

(4) resources needed to sustain the site protection program in its current configuration and during planning revisions;

(5) security staff personnel qualifications as outlined in approved position descriptions and/or prescribed in DOE directives;

(6) the results of vulnerability analyses and risk assessments, including:

(a) levels of acceptable risks,

(b) assumptions established and used as part of the vulnerability analysis process, and

(c) validation of vulnerability analyses results by performance testing.

(7) required corrective actions and how they will mitigate identified vulnerabilities and reduce residual risk;

(8) sources of supporting documentation detailing where planning assumptions, relative to the facility, then adversary, and the DOE national security mission can be found; and

(9) approved deviations.

b. Security Plans. Facilities not required to prepare site safeguards and security plans shall prepare security plans that describe the protection programs in place. In addition, specialized plans shall be developed to address protection programs for classified automated information systems (AIS), materials control and accountability, and other protection operations. Requirements for these specialized plans can be found in the following directives:

(1) Materials Control and Accountability Plans. See DOE 5633.3B, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 9-7-94.

(2) Classified AIS Security Plans. See DOE M 5639.6A-1.

c. Planning Inputs. The following documents shall be used to support program forecasts and information input used in the protection program planning process.

(1) Current DOE directives, DOE threat guidance, and applicable intelligence assessment information developed and disseminated by Headquarters Elements.

(2) Programmatic guidance and forecasts of significant changes planned in site operations, as communicated through Heads of Field Elements and appropriate Headquarters Elements.

(3) Current and projected operational constraints and resources.

(4) Protection program policy guidance provided by DOE Elements.

d. Plan Review and Approval.

(1) Contractors shall provide Site Safeguards and Security Plans, or applicable portions thereof, to Heads of Field Elements for DOE review and approval.

(2) The Site Safeguards and Security Plan shall be reviewed and updated annually. Copies of modifications and updates shall be provided to the Head of the Field Element.

SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. APPLICABILITY. This chapter applies to personnel performing safeguards and security tasks and responsibilities.

2. PROGRAM REQUIREMENTS.

a. The Safeguards and Security Training Program shall encompass training in the following subjects, as applicable:

(1) Program Management.

(2) Personnel Security.

(3) Protection Operations.

(4) Materials Control and Accountability.

(5) Information Security.

b. Training methodology and courses shall be standardized. Development, review, and presentation of training courses for unique site-specific requirements shall be the responsibility of cognizant sites.

c. Training programs shall be based on the results of job analyses to document the identification and description of major tasks and skill requirements.

d. Training shall be provided to individuals to ensure they are qualified to perform assigned safeguards or security tasks or responsibilities.

(1) Initial and refresher training shall be tailored to develop the required knowledge and skills.

(2) The scope and level of training provided to individuals shall be tailored to their assigned duties and responsibilities and shall be based on an analysis of their prior safeguards and security experience and training.

(3) Knowledge and performance-based testing shall apply to all required training to measure the skills acquired from the training programs developed.

(4) For specialized skill requirements, such as armorers, personnel security specialists, nuclear materials custodians, and technical security countermeasures technicians, performance testing shall form the primary basis for certification.

(5) 10 CFR, Parts 1046 and 1048, address certain specific training requirements for protective force personnel.

e. A Training Approval Program (TAP) shall be implemented to standardize safeguards and security training conducted at DOE facilities other than the Safeguards and Security Central Training Academy. (A Training Approval Program Guide will be available to provide details on training standardization.) Site programs shall be examined by Central Training Academy representatives on a recurring basis, but no less than every 3 years, to verify adherence to DOE objectives, standards, and criteria, and to provide program approval recommendations to the Director, Safeguards and Security. Training approvals shall remain valid for 3 years.

(1) Initial and recurring reviews for training approval shall cover all aspects of local training programs, including program management and structure, course contents, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(2) Instructors shall be evaluated for knowledge in assigned training area and effectiveness in presenting assigned course materials.

(3) Individuals shall be tested to evaluate skills and knowledge achieved through course participation.

f. Instructors shall be certified by the individual responsible for the contractor training program. Certification shall remain valid so long as the individual fulfills applicable refresher training. Certification shall be based on a records review of qualifications and a recommendation by the individual responsible for the training program.

g. Covered contractors shall implement a standardized training records management system as described below.

(1) Records shall be maintained to document training provided to personnel participating in the DOE safeguards and security program. Records of training shall contain course identification, dates accomplished, and scores achieved, where applicable.

(2) Records of training provided to individuals shall be retained in electronic or hard copy form. Records shall be retained according to guidance provided in DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95, and General Records Schedules issued by the Archivist of the United States.

(a) Records of training provided at the Central Training Academy shall be maintained at the Academy and shall also be maintained by the organization

sponsoring the individual.

(b) Records of training provided at DOE Elements shall be maintained at DOE Headquarters or the relevant Operations Office, as appropriate, and shall be provided to the organization sponsoring the individual for inclusion in the individual's record file.

(c) Records of training provided at contractor facilities shall be provided to and retained by the organization sponsoring the individual.

(d) Records of training provided at other government or private facilities shall be obtained and maintained by the organization sponsoring the individual.

CHAPTER III

PERFORMANCE ASSURANCE PROGRAM

1. APPLICABILITY. The program focus is on all safeguards and security system elements used to protect Category I and II special nuclear materials and Top Secret matter.

2. PROGRAM REQUIREMENTS.

a. The Performance Assurance Program shall accomplish the following goals.

(1) Provide for operability and effectiveness tests.

(2) Be implemented in a graded manner. Elements that are determined to be most significant are "critical protection elements." Such elements shall be:

(a) identified separately for each facility, based on consideration of the assets being protected, protection system, threat, and vulnerability assessments;

(b) performance-tested, as a minimum, on those scenarios evaluated in vulnerability assessments;

1 Critical protection elements shall be identified and performance tested at least every 365 days. A rationale shall be provided to characterize identified critical protection elements.

2 Critical protection elements shall include elements and/or integrated systems of equipment and hardware, administrative procedures, protective forces, and/or other staff.

b. Performance assurance tests shall be conducted with the highest regard for the safety and health of personnel and protection of the environment, Government property, and national security interests.

c. The adequacy of new and existing protective systems shall be confirmed through testing prior to operational use and periodically thereafter.

(1) Operability tests provide a simple measure of integrity on a frequent basis. Operability testing shall consist of checking the system element or total system to confirm, without any indication of effectiveness, that it is operating. Operability testing intervals may be established based on site-specific conditions and shall be documented in the performance assurance plans.

(2) Effectiveness tests provide comprehensive assurance of integrity on an infrequent basis. Performance testing of equipment for effectiveness shall consist of checking systems to

confirm the satisfactory performance of the required functions over the expected range of use. The frequency of performance testing shall be appropriate to operational needs and threat levels.

d. At least every 365 days, a performance test encompassing protection systems associated with comprehensive site or facility threat scenario shall be conducted to demonstrate overall facility safeguards and security system effectiveness.

3. DOCUMENTATION REQUIREMENTS.

a. Performance Assurance Program Plan. This plan may be an integral part of the Site Safeguards and Security Plan or other security plan, as applicable. The persons, organizations, or groups responsible for corrective actions should be identified. The Performance Assurance Program Plan shall:

(1) describe the program and its administration and implementation;

(2) identify critical protection elements and describe how the performance of these elements is to be ensured, including the manner in which activities performed by external oversight organizations will be applied and interpreted; and

(3) address unsatisfactory results of performance assurance activities, how they are to be captured in the site corrective action program, and how corrections will be implemented.

b. Performance Assurance Reports.

(1) Performance Assurance Reports shall be prepared to document results from field implementation of performance assurance activities.

(2) For evaluations based on tests or oversight activities performed by external organizations, the relevant documentation shall be interpreted and summarized or referenced.

c. Document Retention.

(1) Program and implementation plans, reports, and supporting information shall be retained a provided by law or contract, and/or as long as useful to the program.

(2) Recordkeeping systems shall be capable of providing an audit trail for performance assurance activities and reports.

(3) Disposition of documents shall be in accordance with the DOE Records Management Program.

CHAPTER IV

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. APPLICABILITY. A Safeguards and Security Awareness Program shall be developed, implemented, and maintained at each facility/site/activity having DOE Security Areas, classified matter, and/or special nuclear materials.

2. REQUIREMENTS: SUMMARY OF SAFEGUARDS AND SECURITY AWARENESS PROGRAM.

a. As a condition for unescorted access to DOE Security Areas and/or access to classified information or special nuclear materials, contractor employees (and other individuals granted DOE access authorization) shall receive briefings as required by this chapter.

b. Individuals granted DOE access authorizations shall be precluded or restricted from access to DOE Security Areas, classified information, or special nuclear materials until the briefing requirements of this chapter have been satisfied.

c. Briefings. Safeguards and security awareness programs shall include, but are not limited to, the development and presentation of four briefings.

(1) Initial Briefing.

(2) Comprehensive Briefing.

(3) Refresher Briefing.

(4) Termination Briefing.

d. Topics. Safeguards and security awareness programs shall incorporate the dissemination of information concerning the following.

(1) Applicable DOE safeguards and security regulations, directives, procedures, and guides.

(2) Site-specific (and/or operations-specific) safeguards and security policies, procedures, and requirements.

(3) Other matters of safeguards and security interest, such as:

(a) recent espionage cases,

(b) approaches and recruitment techniques employed by foreign intelligence services,

(c) safeguards or security incidents and considerations,

(d) safeguards or security threats and vulnerabilities, and

(e) classified information. If the discussion of briefing topics involves the exchange of classified information, the presentation must be limited to individuals who possess a DOE access authorization or other agency security clearance.

e. Initial Briefing.

(1) Individuals approved for unescorted access to Security Areas shall receive initial briefings.

(2) Briefing topics shall include, but are not limited to:

(a) overview of DOE safeguards and security disciplines, including personnel security, information security, and physical security;

(b) local access control procedures and escort requirements;

(c) protection of Government property;

(d) prohibited articles; and

(e) reporting of incidents of safeguards and security concern.

f. Comprehensive Briefing.

(1) Prior to being granted access to classified information or special nuclear materials,

individuals granted DOE access authorizations shall receive comprehensive briefings to inform them of their safeguards and security responsibilities. When such individuals are assigned to another DOE facility, they shall receive comprehensive briefings at the new facility.

(2) Briefing topics shall include, but are not limited to, the following.

(a) Information Security.

(b) Physical Security.

(c) Personnel Security.

(d) Reporting/Notification Requirements.

(e) Legal and administrative sanctions imposed for incurring a security infraction or committing a violation.

(f) General information concerning the protection of special nuclear materials.

g. Refresher Briefings. Individuals who possess DOE access authorizations shall receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities. Refresher briefings are mandatory for all individuals possessing DOE access authorizations and shall be implemented each calendar year at approximately 12-month intervals.

h. Termination Briefings. Individuals shall receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing shall be implemented on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information or special nuclear materials, whichever is sooner. Termination briefings shall be based on the information contained in DOE F 5631.29, "Security Termination Statement," and Standard Form 312 (SF-312), "Classified Information Nondisclosure Agreement."

i. Safeguards and Security Awareness Coordinator. The contractor shall appoint a Safeguards and Security Awareness Coordinator who shall formulate and/or maintain a safeguards and security awareness program.

3. DOCUMENTATION REQUIREMENTS.

a. Recordkeeping. Records shall be maintained in a manner that identifies all individuals who have received briefings by type and date of briefing and calendar date. Recordkeeping systems shall be capable of providing an audit trail.

b. Documentation.

(1) A completed SF-312 may serve as the documentation for the comprehensive briefing.

(2) In recurring requirements, such as the refresher briefing, records shall be maintained until the next occurrence of the briefing.

(3) The completion of DOE F 5631.29 satisfies documentation requirements for the termination briefing.

CHAPTER V

FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. APPLICABILITY. This chapter applies to safeguards and security activities involving access authorizations, classified information, nuclear or other hazardous material that presents a potentia radiological or toxicological sabotage threat, and/or Departmental property with a value of $5,000,000 or more.

2. REQUIREMENTS: GENERAL.

a. Nuclear and other hazardous materials presenting a potential radiological or toxicological sabotage threat, classified matter, and property protection interests shall not be permitted on premises occupied by the Department or its contractors until facility clearance is granted.

b. Safeguards and security activities involving access authorizations shall be registered to assist i ensuring proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

c. If no need exists for a contractor's office locations to receive, process, reproduce, store, transmit, or handle classified information or nuclear material, but access authorizations are required for the contractor to perform the work within DOE-approved facilities, the contractor (identified as a non-possessing facility) must be registered. As used in this Contractor Requirements Document, the term facility clearance refers to both possessing and non-possessing facilities.

d. Facility clearance shall be based upon a determination that satisfactory safeguards and securit can be afforded the safeguards and security activities. The determination of a valid facility clearance shall be based upon an approved safeguards and security plan, results of surveys, an a favorable FOCI determination, as appropriate.

e. Approval for other Federal agency safeguards and security activities to be conducted at Department-owned or -operated facilities shall be based on a determination that the safeguard and security measures to be provided are consistent with Departmental policy.

f. Facility clearance for work-for-others safeguards and security activities at other than Department-owned or -operated facilities that are channeled through a Departmental entity shall be based on the validation of the other agency's facility clearance.

(1) Before commencement of non-DOE funded work, conduct, as required by DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, a review of the work request and certify that the sponsoring organization has either provided the appropriate classification guidance or has stated in writing that the non-DOE funded work will not entail classified activities.

(2) Ensure, prior to commencement of the non-DOE funded work involving access authorization, that safeguards and security activities have been recorded as security interests on DOE F 5634.2, "Contract Security Classification Specification," or DD F 254, "Contract Security Classification Specification."

(3) Ensure, before acceptance of any work for another Federal agency, that appropriate reimbursement for safeguards and security costs is negotiated.

3. REQUIREMENTS: FACILITY CLEARANCES.

a. Granting Approval. Approval of a facility is based on the following.

(1) A favorable foreign ownership, control or influence (FOCI) determination, in accordance

with Chapter VI of this contractor requirements document.

(2) A Facility National Agency Check, which has been requested or completed on those facilities that do not possess a Department of Defense (DOD) facility clearance, in accordance with this chapter.

(3) For contractors, contract(s) containing appropriate security clauses.

(4) Approved safeguards and security plans, as appropriate.

(5) If nuclear materials are involved, an established Reporting Identification Symbol code for Nuclear Materials Management and Safeguards System reporting.

(6) For the facility to possess classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or over $5,000,000 of DOE property, not including facilities or land values, at its location, an initial survey or other survey resulting in a report that comprehensively addresses the security interest, conducted no more than 6 months before the facility clearance date, with a composite facility rating of satisfactory.

(7) Appointment of a Facility Security Officer and, if applicable, Materials Control and Accountability Representative. The Facility Security Officer must possess a personnel clearance equivalent with the facility clearance.

(8) Access authorizations for appropriate personnel. Key management personnel must be determined case by case. Key management personnel must be cleared to the level of the facility clearance. Other officials, to be determined by the Lead Responsible Office, must possess appropriate access authorization for classified information or special nuclear materials.

b. Accepting a Contractor's Existing Federal Agency Facility Clearance. A contractor facility holding facility clearance from another Federal agency may be approved by DOE for processing, using, or storing classified matter, contingent upon the actions required by DOE O 470.1.

4. REQUIREMENTS: FACILITY DATA AND APPROVAL RECORD. A DOE F 5634.3, "Facility Data and Approval Record," shall be prepared by the procurement request originator, who forward the completed form, through their own safeguards and security organization, to the cognizant Departmental safeguards and security organization.

a. If a subcontract is established between a DOE prime contractor and another contractor for work involving access authorizations, classified matter or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, it is the responsibility of the prime contractor to ensure the proper preparation of a DOE F 5634.3.

b. The prime contractor is responsible for forwarding information on the DOE F 5634.3 requiring updating to the cognizant Departmental safeguards and security organization.

5. REQUIREMENTS: CONTRACT SECURITY CLASSIFICATION SPECIFICATION.

a. New Activity. If a new activity for work involving access authorizations is being considered, the DOE F 5634.2 (or the DD F 254, "Contract Security Classification Specification") must be submitted by the procurement request originator to the Contracting Officer's Representative.

b. Preparation. A DOE F 5634.2 shall be initially prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental Element Safeguards and Security organization. If a DD Form 254, "Contract Security Classification

Specification" has been used by the agency sponsoring the activity, it shall be annotated with the facility code and submitted instead of the DOE F 5634.2.

CHAPTER VI

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. APPLICABILITY. Foreign ownership, control, or influence (FOCI) determinations are required of the following.

   a. Contractors, which include any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government for the purpose of performing under a contract, license, or other arrangement that requires access authorizations. This includes subcontractors of any tier, consultants, agents, grantees, and cooperative agreement participants.

   b. All tier parents, if the contractor is owned or controlled by another firm(s).

2. REQUIREMENTS.

   a. A facility clearance, which includes a FOCI determination, can only be requested for the successful offeror/bidder if insufficient lead time is expected between selection and contract award to allow deferral of the review.

   b. Contractors shall submit to the Contracting Officer information and documentation that define the extent and nature of any foreign ownership, control, or influence over the contractor and, if applicable, tier parents.

   c. Contractors and any tier parents, subject to the FOCI requirements must submit the following to the Lead Responsible Office:

      (1) Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI representation and certification.

      (2) Complete, current, and accurate information, certifications, and explanatory documentation that define the extent and nature of any relevant FOCI whenever:

         (a) there is any change in ownership or control,

         (b) 5 years have elapsed since the previously provided FOCI representation and certification were executed, or

         (c) the Lead Responsible Office advises that it considers that a relevant change in the nature of the FOCI has occurred.

      (3) Written notification of anticipated changes that include, but are not limited to, the following:

         (a) action to terminate the contractor organization or any of its parents for any reason;

         (b) imminent adjudication of or reorganization in bankruptcy of the contractor organization or any tier parents;

         (c) discussions or consultations with foreign interests that may reasonably be expected to lead to the introduction or increase of FOCI; or

         (d) negotiations for the sale of securities to a foreign interest that may lead to the

introduction or increase of FOCI.

3. REQUIREMENTS: REPORTING SIGNIFICANT CHANGES. When a changes in the extent and nature of FOCI that would affect the information in a contractor's and/or any tier parents' most rec DOE FOCI submission(s) has occurred, the contractor/parent shall immediately provide written notification and supporting documentation relevant to the changes to the DOE Lead Responsible Office. A significant FOCI increase/change that warrants processing of the contractor/parent for a new FOCI determination includes, but is not necessarily limited to, the following.

   a. A new threshold or factor that did not exist when the previous determination was made (e.g., a "no" answer changes to a "yes" answer), and any additional factors associated with the questions on the FOCI representation and certification.

   b. A previously reported threshold or factor that was favorably evaluated by the Lead Responsible Office has increased to a level requiring a determination by the Office of Safeguards and Security.

   c. A previously reported financial threshold or factor that was favorably evaluated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location or end user (i.e., for revenue) or lenders (i.e., indebtedness).

   d. A previously reported foreign ownership threshold or factor that was favorably evaluated by the Office of Safeguards and Security has increased to the extent that a method of negation or reduction is necessary.

   e. Any changes in the ownership or control of the contractor and/or any tier parents.

4. REQUIREMENTS: METHODS TO NEGATE OR REDUCE UNACCEPTABLE FOCI. The affected U.S. organization(s), or its legal representatives may propose a plan to negate or reduce unacceptable FOCI, but the primary responsibility for approving such a plan rests with the Office of Safeguards and Security. A plan may consist of one or more of the insulating measures identified DOE O 470.1, Chapter VI.

5. REQUIREMENTS: ANNUAL CERTIFICATION.

   a. At the end of each year of operation, the Trustees, Proxy Holders, or other principals, as appropriate, shall submit to the Lead Responsible Office an annual implementation and compliance report. Failure of the cleared U.S. organization to ensure compliance with the terms of the applicable security arrangement may result in the organization's facility clearance being suspended pending resolution of the FOCI.

   b. Each contractor holding a facility clearance shall certify annually to the Lead Responsible Office that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

   c. When the contractor is controlled by parent organizations that have been excluded, the contractor must also provide annually to the Lead Responsible Office written certification from an authorized official from each such excluded parent that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization's ownership; and (iii) no changes have occurred in the organization's officers, directors, and executive personnel.

CHAPTER VII

INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. APPLICABILITY.

   a. When an inquiry establishes credible information that fraud, waste and/or abuse has occurred, which does not involve a national security interest has occurred, the Office of the Inspector General shall be notified for information and/or action.

   b. When an inquiry establishes that a potential compromise or unauthorized disclosure of classified information, the applicable provision of DOE O 471.2, INFORMATION SECURITY PROGRAM, shall be followed.

   c. Employees with information indicating possible fraud, waste, abuse, or other forms of wrongdoing in the Department's programs or operations shall inform the Inspector General immediately upon obtaining such information.

2. REQUIREMENTS.

   a. Loss, compromise, or unauthorized disclosure of classified information, and alleged or suspected violations of laws pertaining to safeguards and security shall be reported promptly through the appropriate DOE Element to the Office of Safeguards and Security, Secretarial Officer, and when appropriate, the local Federal Bureau of Investigation office.

   b. Unclassified reports and notifications of safeguards and security incidents shall be made in accordance with DOE O 232.1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION; and DOE O 471.2, INFORMATION SECURITY PROGRAM. Reports which contain classified information shall contain all of the information required by DOE O 232.1, but shall not be entered on the Occurrence Reporting and Processing System. Classified reports shall be sent by approved methods for transmitting classified information. Reporting intervals for incidents of safeguards and security concern must be in accordance with DOE O 232.1.

   c. Federal Bureau of Investigation personnel shall be admitted to areas and afforded access to Restricted Data or other classified information as necessary for them to perform their duties. Such personnel shall be provided escort, as necessary, for safety reasons or to facilitate the investigative progress.

   d. When Federal Bureau of Investigation personnel are given access to classified information, they will be immediately advised of the classification and the category of the information. Appropriate document and data classification, marking information, and protection and control requirements shall be made available to them through local liaison channels.

CHAPTER VIII

CONTROL OF CLASSIFIED VISITS PROGRAM

1. APPLICABILITY. The requirements in this chapter apply to contractor personnel who visit DOE facilities that entail access to classified information.

2. REQUIREMENTS: CLASSIFIED VISIT PROCEDURES. A contractor's basic procedures for the control of all classified visits to DOE facilities shall ensure the following.

   a. Verification of the identity, access authorization (security clearance), and need-to-know of the visitor.

   b. Observance of limitations on access to classified information or facilities.

c. Timely notification (10 days) of visits.

d. Prompt transmittal of "Request for Visit or Access Approval" (DOE F 5631.20), when applicable. (This form is no longer required for DOE and DOE contractor employees who visit DOE facilities. These employees may use their DOE picture identification badge as evidence of a DOE access authorization. However, DOE F 5631.20 is still required for programmatic approval for sigma access and for employees of other Federal agencies who visit DOE facilities.)

e. Timely notification to those concerned for approval of access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by Headquarters Elements.

f. Use of continuing visitor access approval as necessary for individuals who visit DOE facilities frequently. This approval cannot exceed a period of 1 year, but the approval may be renewed annually, if necessary.

g. Operational approval of visits.

h. Maintenance of records of all classified visits by non-DOE personnel and foreign nationals.

i. Referral to the Director of Public and Consumer Affairs of any nonroutine, written, or visual material proposed for public release resulting from visits.

3. REQUIREMENTS: CLASSIFIED VISITS BY DOE EMPLOYEES, CONTRACTORS AND SUBCONTRACTORS.

a. The visitor is responsible for making administrative arrangements and obtaining approval from the Field Element or Secretarial Officer, as appropriate. (The authority granting such approval is responsible for informing the office to be visited.)

b. When the amount of visitor traffic between DOE contractor or subcontractor facilities due to mutual program interests is significant, contractors or subcontractors may be authorized, subject to the limitations in subparagraph c below, to arrange for the visits without obtaining DOE approval if such authorization will be advantageous to DOE.

c. The following procedures are required when access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or specific facilities designated by Headquarters Elements having program direction is required.

(1) A determination of the need for access shall be made by the DOE official sponsoring the visit.

(2) Approval of the access during visits under the auspices of a Headquarters Element should be obtained from the Headquarters Element exercising jurisdiction over the facility or office to be visited.

(3) Approval of this access during visits under the auspices of Field Elements shall be obtained from the responsible Field Element for field visits, and for visits to Headquarters, from the organization being visited.

4. REQUIREMENTS: VISITS TO DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION FACILITIES.

a. A DOE F 5631.20 shall be forwarded directly by contractors, through DOE Elements, to the commanding officer or the director of the facility after first verifying the visitor's clearance at the DOE Element.

b. DOE Top Secret approvals shall be specifically certified in the event access to Top Secret information is required.

c. Any exchange of Restricted Data occurring during the course of the visit shall be accomplished as stated in paragraph 7 below.

5. REQUIREMENTS: RESTRICTED DATA VISITS BY NUCLEAR REGULATORY COMMISSION EMPLOYEES.

a. Visits to DOE facilities by Nuclear Regulatory Commission employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology, or entry into a DOE classified weapon or production facility shall:

(1) be arranged through the respective Headquarters Element that will coordinate the visits;

(2) if to classified weapon or production facilities, have prior approval of the Assistant Secretary for Defense Programs; and

(3) have DOE F 5631.20 or the Nuclear Regulatory Commission equivalent with necessary clearances certified by the Director of Security, Nuclear Regulatory Commission.

b. Visits involving access to other Restricted Data not requiring prior approval from the appropriate Headquarters official exercising jurisdiction over the facility or office to be visited may be arranged directly by Nuclear Regulatory Commission with the cognizant DOE Element, provided this procedure does not conflict with the existing visitor control procedures of the division or office having program responsibility. A DOE F 5631.20 or Nuclear Regulatory Commission equivalent is required.

c. The Nuclear Regulatory Commission identification badge shall not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

6. REQUIREMENTS: RESTRICTED DATA VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES.

a. Access to Restricted Data is contingent upon submission of a DOE F 5631.20, National Aeronautics and Space Administration Form-405, "Request for Access Approval," or a memorandum or electronic message signed by or in the name of the certifying official. The request shall be forwarded for approval or other action to the DOE official with jurisdiction over the information to which access is desired.

b. The request for access shall include the following:

(1) Name(s) of person(s) and organization represented (if not Armed Forces, relationship to the Department of Defense or National Aeronautics and Space Administration).

(2) Information to which access is desired. Access to critical nuclear weapon design information must be specified when it is required.

(3) The security clearance or access authorization status of each person.

(4) Certification that the person needs the access in the performance of duty.

(5) Anticipated date of visit and names of persons to be visited, as appropriate (if a conference is involved, the date, place, and sponsor of the conference shall be specified).

(6) Statement of determination that permitting the person(s) access will not endanger the common defense and security.

(7) Citizenship and date of birth.

(8) For requests from National Aeronautics and Space Administration, a certification that the matter to which access is desired relates to "aeronautical and space activities."

c. The approving official must possess or have been delegated the authority to approve such access. The approving official must satisfy himself/herself:

(1) as to person's identity,

(2) that the person's clearance or access authorization is at least equal to the classification of the information to which access is desired.

d. Access to Restricted Data in the custody of DOE contractors and subcontractors may be authorized by Heads of DOE Elements in accordance with the following:

(1) The person's identity has been established.

(2) The person's clearance or access authorization, as indicated in the request, is at least equa to the classification of the information to which access is desired.

(3) Access to certain programs or information is handled in accordance with the following:

(a) Weapons Production Programs. For access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, the requests shall be referred to the Assistant Secretary for Defense Program.

(b) Uranium Enrichment. For access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the request shall be referred to the Office of Uranium Programs.

(c) Naval Nuclear Propulsion Information. When access is desired to Naval Nuclear Propulsion Information, the request shall be referred to the Office of Naval Reactors.

e. Control of access by members of the Armed Services or Department of Defense or National Aeronautics and Space Administration personnel or contractors to Restricted Data in the custody of another Federal agency is the responsibility of the appropriate official or his/her designee named in DOE O 470.1. Federal officials named are responsible for maintaining a central index to record access approvals.

7. REQUIREMENTS: OTHER CLASSIFIED VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES .

a. Requests for such visits to contractor and subcontractor facilities are approved by Heads of Field Elements or, in the case of Headquarters Elements, by the head of the element concerned after assuring that such visitor possesses appropriate military or National Aeronautics and Space Administration security clearance and requires the information in the performance of his/her duties.

b. Certification of security clearance may be made by memorandum, electronic message, DOE F 5631.20, or National Aeronautics and Space Administration Form 405.

8. REQUIREMENTS: CLASSIFIED VISITS BY EMPLOYEES OF OTHER FEDERAL AGENCIES.

a. Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than the Department of Defense, National Aeronautics and Space Administration, or Nuclear Regulatory Commission are approved by the Field Elements or, for Headquarters, by the organization concerned.

b. Restricted Data may not be exchanged with persons in this category unless they possess appropriate DOE access authorization.

c. Classified information other than Restricted Data may be exchanged with such individuals if they possess Q or L access authorizations or security clearances under the provisions of Executive Order 10450, "Security Requirements for Government Employment," and require the information in the performance of their duties.

9. REQUIREMENTS: CONGRESSIONAL AND STATE CLASSIFIED VISITS.

a. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by Governors or their staffs may be approved by Heads of DOE Elements provided the following are established.

(1) The visitors' identities.

(2) Access authorization or security clearance.

(3) "Need-to-know."

b. The Assistant Secretary for Congressional and Intergovernmental Affairs shall be advised of requests and action taken on the requests for such visits.

10. REQUIREMENTS: EMERGENCY VISITS TO CLASSIFIED AREAS AND FACILITIES.

a. In an emergency, requests for visit approval may be made by telephone or electronic message

b. Telephonic requests must be confirmed by memorandum or electronic message.

11. REQUIREMENTS: CLASSIFIED VISITS BY FOREIGN NATIONALS TO DOE FACILITIES.

a. Visits by foreign nationals possessing Department of Defense or National Aeronautics and Space Administration security clearances will be arranged in accordance with paragraph 6 above.

b. Visits by foreign nationals possessing security clearances granted by Federal agencies other than the DOE, Department of Defense, or National Aeronautics and Space Administration shall be arranged in accordance with paragraph 7 above.

c. Visits by foreign nationals who are sponsored by a foreign government shall be arranged as follows.

(1) If the visit is in connection with the military application of atomic energy under sections 144b and c(1) and 91c(1) or (4) of the Atomic Energy Act of 1954, as amended, the Assistant Secretary for Defense Programs shall make all arrangements for the visit,

including appropriate approvals and security assurances.

(2) If the visit is to the Office of Declassification in connection with the information classification program under DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, the Director of Declassification shall make arrangements for the visit, including appropriate approvals and security assurances.

(3) If the visit is not in connection with programs covered in the above paragraphs, the Deputy Assistant Secretary for International Energy Policy shall arrange for the visit in concert with the appropriate Headquarters staff other than those listed above, and shall coordinate with the Director of Safeguards and Security for the necessary security assurances.

(4) If the visit is in connection with naval nuclear propulsion matters, the Director of Naval Reactors shall make arrangements for the visit, and shall have the Director of Safeguards and Security obtain the necessary security assurances.

(5) Security assurances received under the above paragraphs shall be retained for 5

SURVEY PROGRAM

1. APPLICABILITY. The Survey Program applies to all facilities that are eligible to have access to, use, store, or transmit nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat and/or classified information, that require access authorizations, or th possess over $5,000,000 of DOE property, exclusive of facilities and land values.

2. REQUIREMENTS: CORRECTIVE ACTIONS.

a. When a survey contains findings, the surveyed organization shall submit a response identifying corrective action(s) for each finding to the Responsible and Surveying Offices no later than 30 working days after the formal receipt of findings. The corrective action(s) should be based on documented root cause analysis, risk assessment, and cost-benefit analysis.

b. Contractors shall provide quarterly reports of corrective action(s) for each finding to the Responsible and Surveying Offices. CHAPTER X

SELF-ASSESSMENT PROGRAM

1. APPLICABILITY. This program applies to contractor facilities for which a DOE F 5634.3, "Facility Data and Approval Record," is recorded. The level of detail of the self-assessment may be specifie by the Lead Responsible Office.

2. REQUIREMENTS.

a. Self-assessment programs shall be conducted and documented for all cleared facilities. The self-assessment program shall:

(1) include reviews of all applicable DOE F 5634.1, "Safeguards and Security Survey Report," topical and subtopical areas of the facility's safeguards and security program/system;

(2) be conducted between the periodic surveys conducted by the Surveying Office; and

(3) be conducted using personnel knowledgeable of the programmatic or topical area.

b. Self-assessment reports shall:

(1) address reviewed topical areas;

(2) be used as organizational management tools/aids in determining the status of safeguards and security performance and compliance with applicable safeguards and security order requirements;

(3) be available for review by the Surveying Office during surveys; and

(4) list findings resulting from self-assessment activities.

c. Findings resulting from self-assessments shall be processed as follows:

(1) Reviewed during the surveys by the Surveying Office.

(2) Addressed by facility/organization management through a documented corrective action plan.

(3) Reviewed and the status of findings tracked until closed.

(4) Reported to the Lead Responsible Office if:

(a) a vulnerability to national security, classified information, nuclear materials, or Departmental property results, or may result, in a significant anomaly that could have significant programmatic impact or embarrass the Department; or

(b) the self-assessment is used to extend the Surveying Office's periodic survey frequency.

(5) be documented in survey reports when deficiencies still exist and have not been adequatel addressed.

DEVIATION REQUEST FORMAT

1. Date. Date the request is signed by the requesting official.

2. Request Number. Alphanumeric identifier beginning with "OSS," followed by the routing symbol used in the DOE National Telephone Directory, followed by the last two digits of the year in the request's date, followed by the three-digit number that is next in the sequence of requests from th Field Element in that calendar year. For example, the third request from Albuquerque Operations Office during 1995 would be OSS-AL-95-003.

3. Directive Citation. Title and date of the directive from which a deviation is being requested with a citation (paragraph or other provision) and summary of the directive's requirement.

4. Impacted Entity. Identification of the specific facility (Safeguards and Security Information Management Systems facility code number), process, procedure, system, etc.

5. Deviation Justification. Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the subject of the deviation request t other safeguards and security interests shall be included if they are significantly affected.

6. Protection Measures. Description of the current measure(s) used for protection and an evaluation the effectiveness of such measure(s); description of alternate/compensatory measure(s) or level(s

protection to be provided as an alternative to the Order requirement(s).

7. Duration. Expected duration of the condition for which the deviation is requested, including milestones for correcting, alleviating, or eliminating the deviant condition, if applicable. (Note: Waivers cannot be for more than 2 years; exceptions cannot be for more than 3 years.)

8. Risks. Evaluation of the risk associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternative(s) shall be included.

9. Signature. Requesting official's signature.

U.S. Department of Energy PAGE CHANGE
Washington, D.C.

6-21-96

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. PURPOSE. To transmit revised pages to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM, of 9-28-95.

2. EXPLANATION OF CHANGES. To clarify that persons seeking unescorted access to security areas must receive an initial briefing, and sign the Classified Information Nondisclosure Agreement before access to classified information is granted. In addition, a Manual to supplement this Order will be published in lieu of a Guide.

3. FILING INSTRUCTIONS.

a.	Remove Pages	Dated	Insert Pages	Dated
	IV-I to IV-4	9-28-95	IV-1 to IV-4	6-21-96

b. After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Human Resources

and Administration

Related Documents

DOE O 470.2A Text Version PDF Version

DOE N 470.2 Text Version PDF Version

DOE P 470.1 Text Version PDF Version

This site sponsored by the Office of Management & Administration of the US Department of Energy.

Operated by Innovative Web Applications, Inc. and Powered by explorit

6

Department of Energy
Germantown, MD 20874-1290

95-5634.1B-0067

MAR 28 1995

MEMORANDUM FOR DISTRIBUTION

FROM: EDWARD J. MCCALLUM
DIRECTOR, OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: REPORTING AND TRACKING OF SURVEY FINDINGS AND CORRECTIVE ACTIONS

Attached is updated guidance on reporting and tracking of survey findings and corrective actions. The only significant change is the reduction of codes to be used for recording and tracking findings in the Safeguards and Security Information Management System (SSIMS). The guidance provides standardization and will improve the quality of the data in the SSIMS. The finding numbers are now system-generated upon entry of a finding into the SSIMS.

The attached guidance supersedes that provided in my memoranda, "Portion Marking for Department of Energy (DOE) Safeguards and Security Survey Findings and Corrective Actions," dated December 22, 1992, and "Office of Safeguards and Security (OSS) Tracking of Survey Findings and Corrective Actions," dated January 31, 1994, both of which are hereby rescinded. The attached guidance will be incorporated in the Safeguards and Security Survey and Self-Assessment Guide, when published.

If you have any questions regarding the attached guidance, please contact Cathy Tullis on (301) 903-4805.

Attachment

cc:
FSA Quality Panel

Printed with soy ink on recycled paper

REPORTING AND TRACKING OF SURVEY FINDINGS AND CORRECTIVE ACTIONS

I. GENERAL.

Three copies of each survey report must be sent to the Assessment and Integration Branch, Field Operations Division, Office of Safeguards and Security.

Only the terms Findings and Suggestions will be used in the survey program. Findings and all other statements that need to be emphasized, such as observations of conditions, are to be contained in the narrative sections of the report. Where practical, suggestions (program enhancements) should be listed and identified as distinct items or as a separate paragraph at the end of the narrative for each safeguards and security topical area delineated on DOE Form 5634.1, Safeguards and Security Survey Report.

The Safeguards and Security Information Management System (SSIMS) serves as the central tracking database for findings of surveys and other inspection activities. Each Operations Office is responsible for entering and providing corrective actions on survey findings, including findings from Technical Surveillance Countermeasures (TSCM) surveys. The Surveying Office is responsible for entering all findings into the SSIMS; the Lead Responsible Office, for reporting of the status of corrective actions for the findings.

Findings shall be monitored and the status of the corrective actions shall be reported to SSIMS until resolved. This includes findings of all surveys, inspections, reviews, or evaluations (including, but not limited to, Headquarters Program Reviews, Field Element Surveys, Automated Information System Security Surveys, TSCM Surveys, Security Evaluations, Inspector General, and General Accounting Office Reports).

The tracking of findings is the responsibility of the Surveying Office and the Lead Responsible Office. When the Surveying Office is different from the Lead Responsible Office, timeliness and documentation of findings and ratings is critical. The Surveying Office must notify the Lead Responsible Office of findings. Similarly the Lead Responsible Office must keep the surveying organization appraised of findings status.

NOTE: Findings may be assigned to an office other than the Lead Responsible Office if they are specific to the other office's interests.

II. PORTION MARKING

Each finding and subsequent corrective actions will be required to have a stand-alone security classification (i.e., SRD, SNSI, SFRD, CNSI, U, etc.). Paragraphs and portions thereof are required to be marked with the highest classification level and category of the information contained therein. This requirement includes Restricted Data (RD), Formerly Restricted Data (FRD), and National Security Information (NSI).

III. SYNOPSIS OF FINDINGS

Findings shall be documented in each survey report and listed separately in an Executive Summary or at the end of the report. The data for each finding should include: (1) the Finding Number, (2) the Finding Synopsis, (3) the Classification of each finding, (4) the DOE Order Reference Number, and (5) the Standards and Criteria Reference Number. Including the Standards and Criteria Reference Number is optional.

Each finding will be described in a synopsis format (FINDING SYNOPSIS). The SSIMS allows a maximum of 500 alpha/numeric characters and spaces. Each finding is to have a separate, stand-alone classification level and category at the end of the finding synopsis statement. A separate five-character field is provided for the finding classification in the SSIMS.

Each finding is to have an alpha/numeric reference to the DOE Order that identifies the requirement not being met in the finding. This reference should be written as DOE Order XXXX.XX; followed by the chapter, section and sub-section reference numbers and/or letters, e.g., 5632.1C, II.A.3.c.

Each finding is to have an alpha/numeric reference to the safeguards and security Standards and Criteria that identify the requirement not being met in the finding. This reference should be written as the topical area (PM, PPO, IS, NMCA or PS) followed by the numeric reference to the section and sub-sections.

IV. SURVEY REPORT FORM

A fully completed Safeguards and Security Survey Report Form (DOE F 5634.1) will be used to document each survey and will accompany each narrative survey report. The ratings rendered shall be annotated as **S**, **M**, or **U** (for **S**atisfactory, **M**arginal or **U**nsatisfactory) only. Those areas not applicable to the surveyed facility shall be rated **DNA** (for **D**oes **N**ot **A**pply). Any other notations (such as NR, for not rated) are not acceptable.

NOTE: The **DNA** rating means that the topical/subtopical program element was not required to be implemented at the surveyed facility. It may not be used in facilities where the program element is mandated but, for whatever reason, was not surveyed. All mandated programs must be surveyed and rated **S**, **M**, or **U**. Only programs not required may be omitted from the survey and rated **DNA**. For example, a facility that has no classified automated information systems would have a **DNA** rating for the Classified AISS subtopical element. If, however, the facility has, or is approved for, classified automated data processing, the Classified AISS element must be surveyed and a rating of **S**, **M**, or **U** must be assigned this subtopical element. If separate surveys are conducted to review topical areas, the Surveying Office is responsible for consolidating the survey ratings on a single DOE F 5634.I.

V. FINDING NUMBERING SYSTEM

Each finding identified in the survey report must have a unique identification number assigned, which must be used throughout the reporting and tracking

process. The following number system is mandated, in order to provide consistency in the SSIMS. A number in this format will be system-generated upon entry of the finding into the SSIMS.

EXAMPLE FINDING NUMBER: 90MAR10-HQS-0515-SSIS-PM-010

A. The date of the survey. The last date of the survey is used if the survey occurred over several days. The date will be written in the following format: two numeric digits for the year (YY); three alpha characters for the month (MMM); and two numeric digits for the day of the month (DD).

B. Two or three alpha characters for the Lead Responsible Office or other office assigned responsibility for the oversight/tracking of the corrective action(s) for the deficiency, not the Surveying Office, unless they are the same.

C. The facility code for the subject facility written with four numeric digits. A "0" should precede all three digit numbers.

D. Up to five alpha characters designating the source/type of report. The following codes are those used as source/type identifiers in the SSIMS:

CODE	TYPE OF DOCUMENT OR ORGANIZATION
GAO	General Accounting Office Reports
IG	Inspector General Reports
OSE	Security Evaluations Inspections
SPEC	Special Surveys
SSIS	Safeguards and Security Initial Surveys
SSPS	Safeguards and Security Periodic Surveys
SSTS	Termination Surveys
TSCM	TSCM Reports

All safeguards and security periodic surveys now fall within the code "SSPS." The codes "NMS" and "PROP" have been deleted. These surveys shall be entered as an initial, periodic, or termination survey, as appropriate.

A Special Survey would be a survey conducted at the facility and/or activity for a specific purpose, such as a review of a security system, a detailed review of a problem area, an unannounced survey, shipment of nuclear materials or classified material, or change in the contractor operating a government-owned facility. A special survey may be predicated on a new security interest or significant configuration change, the need to review or validate corrective actions, or other special, out-of-cycle survey requirement. These would typically relate to specific S&S interests and would, therefore, likely be more limited in scope than the initial or periodic survey.

E. Up to four alpha characters which designate the topical area surveyed. The following codes should be used:

PM	Program Management
PPO	Protection Program Operations
IS	Information Security
NMCA	Nuclear Materials Control and Accountability
PS	Personnel Security

F. Up to three numeric digits designating the sequential number of an individual finding within the topical areas listed above.

VI. CORRECTIVE ACTIONS AND QUARTERLY REPORTS

Upon presentation of a finding at the survey close-out, the facility is to take appropriate corrective measures and/or identify measures to be taken, including milestones for completion. Identification of corrective actions can be accomplished in a timely manner through a documented agreement and commitment for corrective action that the facility, Surveying Office, and other appropriate individual(s) (such as the Contracting Officer) sign at the time of close-out; OR the facility can identify corrective actions, including milestones for completion, to the Lead Responsible Office, not later than 30 days after receiving the survey report. The Lead Responsible Office's initial reporting timeline depends on the overall composite rating assigned to the facility. The Surveying Office will make the initial input of the finding and any identified corrective action, including milestones for completion, to the SSIMS, the Lead Responsible Office, and appropriate Headquarters elements.

Once entered into the SSIMS, the Lead Responsible Office may update the SSIMS daily, but must update the system quarterly. Quarterly status reports for all outstanding findings are required to be submitted to the Lead Responsible Office by the 15th day of the month following the end of the calendar quarter (i.e., January 15, April 15, July 15, October 15). Data is to be entered into SSIMS by the Lead Responsible Office no later than the end of the months of January, April, July, and October. When the quarterly update has been completed, a confirmation shall be forwarded via electronic mail or memorandum to HQ (NN-513.1).

All findings must continue to be reported until validated and a formal closure notification is provided to the facility. Findings cannot be considered closed until associated corrective actions have been verified as completed. A commitment by the facility to implement a corrective action does <u>not</u> constitute completion of that corrective action.

7

DOE/IG-0482

INSPECTION REPORT

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

SEPTEMBER 2000

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

Department of Energy
Washington, DC 20585

September 28, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman /s/
Inspector General

SUBJECT: INFORMATION: Summary Report on "Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process" DOE/IG-0482

BACKGROUND

The Director, Office of Security and Emergency Operations provided the Office of Inspector General with a letter he had received which raised allegations of serious improprieties in the Department of Energy's Site Safeguards and Security Planning (SSSP) process. Specifically, the letter included allegations that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites, and that a contractor's findings under the SSSP Quality Assurance (QA) process were either ignored or not acted upon in a timely manner. In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues. The Office of Inspector General initiated an inspection to evaluate these issues.

RESULTS OF INSPECTION

While the inspection disclosed significant problems in the SSSP process as it was functioning at the time referred to in the allegations, the evidence did not support the principal points raised in the letter. Specifically, the inspection findings did not support the allegations that Department officials:

- lied in the reporting of the actual status of security at the Department's most important nuclear sites; or

- suffered retaliation for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy.

We did find that an employee of a support services contractor believed that an Office of Safeguards and Security program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant to the Secretary. However, the program manager denied making such threats.

We did identify significant problems in the manner in which SSSPs were reviewed and SSSP QA issues were closed during the period referred to in the allegations. Specifically:

- There were substantial differences in what was being reported as the actual status of security at Department sites by the SSSP QA function, and what was being reported by the cognizant sites.

- Final Departmental decisions on how to address the SSSP QA issues were often complicated or delayed by disagreements between field and Headquarters elements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions related to worst case scenarios. These relationships were often so acrimonious as to threaten the effectiveness of the SSSP process.

- Since there was no process to resolve SSSP QA issues in coordination with the SSSP QA function, certain "Risk" issues remained unresolved at the SSSP QA level or were not fully evaluated.

The inspection disclosed that the allegations primarily concerned an SSSP process that has been phased out by the Department. The Office of Security and Emergency Operations is implementing a new process that is intended to address many of the problems that developed during past reviews of SSSPs. We concluded that the Department's restructuring of the SSSP process, if implemented and executed as planned, has the potential for resolving disagreements over the fundamental questions that affect SSSP "Risk" determinations.

This report includes several recommendations for the Director of the Office of Security and Emergency Operations: most notably, to establish a policy on what actions are required once high and moderate risks are identified through the SSSP process; and, to ensure that a dispute resolution process resolves disagreements that occur.

MANAGEMENT REACTION

The Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate. Although the Director has not committed to implementing the inspection recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented.

Attachment

cc: Deputy Secretary
Under Secretary for Nuclear Security/Administrator for National Security
Under Secretary for Energy, Science and Environment
Deputy Administrator for Defense Programs
Director, Office of Security and Emergency Operations
Director, Office of Security Affairs
Director, Office of Safeguards and Security
Director, Office of Defense Nuclear Security
Assistant Secretary for Environmental Management
Manager, Albuquerque Operations Office
Manager, Rocky Flats Field Office
Director, Transportation Safeguards Division
Director, Office of Security Support, Defense Programs

SUMMARY REPORT ON ALLEGATIONS CONCERNING THE DEPARTMENT OF ENERGY'S SITE SAFEGUARDS AND SECURITY PLANNING PROCESS

TABLE OF CONTENTS

Overview

Introduction and Objective 1

Observations and Conclusions 2

Reporting of the Actual Status of Security 2

Actions to Evaluate and Resolve High Risk Concerns 2

No Evidence of "Dumbing" Down the SSSP Process 3

Retaliation 4

Recommendations 6

Management and Inspector Comments 7

Appendices

A. Scope and Methodology 8

B. Background 10

C. Definitions 12

Overview

INTRODUCTION AND OBJECTIVE

In January 2000, the Office of Inspector General received an allegation that there were serious improprieties in the Department's Site Safeguards and Security Planning (SSSP) process. Specifically, it was alleged that a number of people within the Department were "lying in the reporting of the actual status of security" at the Department's most important nuclear sites. Specific allegations were made regarding the Rocky Flats Environmental and Technology Site (RFETS), the Transportation Safeguards Division (TSD), and Los Alamos National Laboratory (LANL). In addition, it was alleged that "illegal" retaliation was taken against those who were trying to correct the Department's security problems through SSSP reviews or through assistance to a special assistant to the Secretary on Department security issues.

Based on these allegations, the Office of Inspector General initiated an inspection to determine if:

- officials within the Department were lying in the reporting of the actual status of security at the Department's most important nuclear sites;
- appropriate actions were taken to evaluate and resolve High Risk concerns;
- there was a systematic pattern of "dumbing" down the SSSP process; and,
- there has been retaliation against those who were trying to correct security problems.

As noted above, this inspection focused on the manner in which the contractor's concerns were addressed by Department security officials once they were raised. The issue of whether or not certain risk conditions actually existed at Department sites, as alleged, was beyond the scope of our review.

OBSERVATIONS AND CONCLUSIONS

REPORTING OF THE ACTUAL STATUS OF SECURITY

The Office of Inspector General found no evidence to support the allegation that Department officials lied in the reporting of the actual status of security at RFETS, TSD, and LANL. Contrary to this allegation, the results of our inspection revealed that Department officials took steps to assure that many of the SSSP QA issues reported by the contractor and the QA function were briefed at the highest levels of Department management.

However, a comparison of the SSSP QA analyses prepared by the contractor, and SSSP correspondence and documentation prepared and approved by the Department's Field and Headquarters Program Offices, did reveal substantial differences in what was being reported as the actual status of security at these three sites. We found that these differences were the result of significant, and, at times, bitter disagreements over the underlying basis of the SSSP QA issues raised by the contractor. The contractor's QA concerns were not well received at the Field Office level, the Program Office level, or by certain elements of the Office of Safeguards and Security. In several instances, the QA analyses performed by the contractor used different assumptions than had been used by the sites to develop their draft SSSPs, creating contention over the contractor's determinations of risk. The risk conditions identified and reported by the contractor were not universally accepted within the Office of Safeguards and Security or by the affected field sites and Program Offices.

ACTIONS TO EVALUATE AND RESOLVE HIGH RISK CONCERNS

Field and Headquarters elements considered and reviewed the QA issues identified by the contractor and the QA function. However, decisions on how to address the QA security concerns were often complicated or delayed by disagreements over fundamental questions such as interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that went into the identification, modeling, and testing of worst case scenarios. For example:

- The contractor and the QA function reported a High Risk concern at a RFETS facility in March 1997. The condition underlying the High Risk concern was not resolved at the QA level for nearly two and one-half years, and the corrective actions taken in October 1999 were still disputed by the site with regard to the necessity for these actions.

Many of the QA issues were briefed within the highest levels of Department management, yet we could not identify a systematic process for resolving and closing the QA issues in coordination with the QA function. As a result, certain issues remained

unresolved at the QA level or were not fully evaluated. For example:

- The contractor and the QA function reported two High Risk scenarios involving TSD operations during its review of TSD's draft September 1998 SSSP. However, the High Risk label was removed from the discussions on one of these issues, and the issue of High Risk in this case was never resolved with the QA function. The Office of Safeguards and Security and TSD did agree to address many of the underlying security concerns that contributed to the QA assertion of High Risk.

- During a limited review of LANL's draft 1999 SSSP, the contractor and the QA function reported that SNM was not at low risk at a LANL facility. However, the issues identified in the contractor's final SSSP QA analysis were not forwarded to the Albuquerque Operations Office or the site for evaluation prior to SSSP concurrence by the Office of Security Affairs.

NO EVIDENCE OF "DUMBING" DOWN THE SSSP PROCESS

We concluded that the "new" SSSP procedures being implemented by the Office of Security and Emergency Operations did not reflect a systematic pattern of "dumbing" down the SSSP process. In fact, we concluded that the new SSSP procedures have the potential for significantly enhancing the SSSP process. Nevertheless, given the Department's past experiences in the security area, strong management involvement will be needed to assure that the "new" process achieves its potential. The Secretary of Energy assigned this role to the Director, Office of Security and Emergency Operations, in June 1999, and stated that the new Director has "the experience, expertise and determination to change the security culture at DOE." This role will have to be re-evaluated in light of the establishment of the National Nuclear Security Administration.

The Department began restructuring the SSSP process in May 1999. The Office of Safeguards and Security believed that the "old" SSSP QA process caused a great deal of contention when Headquarters Offices performed "a post-facto" verification and validation exercise using tools or approaches different than those used to perform the initial risk assessment by the sites. In May 1999, the Under Secretary directed that an SSSP Working Group be formed to provide "new" detailed procedures for the development and approval of SSSPs. The most significant changes from the "old" to the "new" SSSP process was the introduction of a "participatory approach" to the preparation of the SSSPs. The "participatory approach" involves field elements and various Headquarters offices in the SSSP development from the beginning,

eliminating the need for a "post-facto" QA function. Under the "participatory approach," agreement is to be reached on the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios early in the process, thereby avoiding the introduction of different interpretations and assumptions at the end.

The "new" process also introduced a different approach to "Risk." Under the new process, "risk avoidance" was replaced by the concept of "risk management." As described to us, the "new" process emphasizes the necessity of a common, up front agreement on factors that are absolutely critical to the structure of the protection systems designed to counter adversary acts. We concluded that the "new" process must not only move the discussion on the Design Basis Threat, adversary capabilities, and worst case scenarios to the beginning of the SSSP process, but must also provide for the resolution of disputes on these issues when they occur. We also concluded that the "new" process can be most effective if the "Risk" determinations are driven by a consensus within the Department on the interpretation of the Design Basis Threat, adversary capabilities, and worst case scenarios rather than based on the preferences of a single site and/or a Program Office. The Director of the Office of Safeguards and Security told us that "this will be the case."

The inspection disclosed that the "new" process appears to be evolving in a way that will address disputes and the factors affecting "Risk." For example, a newly formed Threat Assessment Quality Panel has assumed responsibility for matters relating to the Design Basis Threat, and any issues not resolved by this panel will be raised to the Security Management Board.[1] In addition, the Threat Assessment Quality Panel has recently issued guidance to Department sites regarding the applicable adversary capabilities under the specific elements of the Design Basis Threat.

The "new" process was first used in April 2000 for the 2000 TSD SSSP. We have not evaluated the effectiveness of this process.

RETALIATION

We found no evidence of retaliation as alleged with respect to Department officials. Interviews of Department officials who were alleged to have been retaliated against for their part in the review of SSSPs, or for assisting a special assistant to the Secretary of Energy on security issues, did not support the allegation of retaliation. However, one support services contractor believed that

[1] The Security Management Board was abolished in October 1999, and a new organization to take over its responsibilities has not been established.

an OSS program manager threatened him with a reduction in contract activity for his role in supporting the SSSP QA process and for assisting the special assistant. The contractor said that he did not receive any contract work in the area of field assistance after the alleged threat was made, and that he viewed the elimination of his field assistance activities as retaliation. However, the OSS program manager denied any retaliation and said that he had no opportunity to provide contract work to this individual during the period in question. Subsequently, the contractor received other contract work, including work from the Director, Office of Security and Emergency Operations, and did not seek to formally address any concerns about alleged retaliation.

We also found no evidence that another support services contractor was retaliated against. The contractor offered a reduction in billable hours as evidence that the contractor was being retaliated against. However, while some Office of Safeguards and Security officials expressed dissatisfaction with the contractor, the use of the contractor by the Office of Safeguards and Security has continued. Office of Safeguards and Security records show that the contractor's billable hours had dropped off significantly in one area, but a review of the contractor's total direct productive labor hours over the past year showed only a slight decline in the overall use of the contractor by the Office of Safeguards and Security.

The evidence shows that the Department's shift from the "old" to the "new" SSSP process, and not retaliation on the part of any OSS official, more likely than not was the cause of this decline. The shift from the "old" to the "new" SSSP process nearly eliminated this company as a support services contractor. However, the contractor's direct productive labor hours have been sustained close to previous levels by providing support in other security areas.

Recommendations

We recommend that the Director of the Office of Security and Emergency Operations:

1. Establish policy on what actions are required once High Risk and Moderate Risk are identified through the SSSP process, including the resolution of High Risk and Moderate Risk issues within specific timeframes; and the consideration for compensatory measures, formal acceptance of risk, and mitigation of risk through operational changes.

2. Ensure that a dispute resolution process is incorporated within the responsibilities of the Threat Assessment Quality Panel and the successor organization to the Security Management Board so that disagreements on the interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios are addressed at the highest level of management.

3. This recommendation is classified.

4. Ensure that TSD validates the Special Response Force through the use of performance testing of the worst case scenarios.

5. Evaluate TSD's performance testing program and assure that all performance tests used to validate their SSSPs (a) are not encumbered by training priorities, (b) constitute legitimate force-on-force activities without coaching by instructors/controller, and (c) provide results that are conclusive in terms of measuring the ability of Special Agents to perform in response to an actual attack.

6. Ensure that TSD validates all other corrective actions that were identified on the "TSD Interim Disposition of NN Comments" matrix.

7. Ensure that TSD identifies a site suitable for conducting force-on-force exercises for worst case scenarios.

8. Evaluate the concern that a "Super Adversary" is created by the application of the Design Basis Threat to worst case scenarios, and determine what action is needed to disseminate more prescriptive policy on adversary capabilities so that the threat and adversary attributes contained in the Design Basis Threat are clear, concise and universally understood by the Office of Security Affairs, Office of Independent Oversight and

Performance Assurance, the Program Offices, and all affected field elements.

It should be noted that certain recommendations originally sent to the Director, Office of Security and Emergency Operations for comment are now the responsibility of the Under Secretary for Nuclear Security/Administrator for National Security.

MANAGEMENT COMMENTS

Officials from the Office of Security and Emergency Operations provided several comments to the initial Draft Report dated July 21, 2000. Appropriate changes were made based on these comments, and a second draft report was issued on August 31, 2000.

In comments provided to the second Draft Report, the Director of the Office of Security and Emergency Operations stated that he had reviewed the Draft Report, and concurred. The Director stated that the conclusions offered in the Draft Report were appropriate, and that it appeared that most of the comments provided by members of the Office of Security and Emergency Operations on the initial Draft Report had been incorporated into this version.

While the Director did not commit to implementing the recommendations, he stated that he would review the relevance of the recommendations in light of other policy initiatives currently underway to ensure that they are complementary. He also stated that if it is determined that the recommendations are appropriate and represent added value to the Site Safeguards and Security Planning Process, they will be implemented. In addition, the Director stated that he would forward to the National Nuclear Security Administration, Office of Defense Nuclear Security, those recommendations that fall under their purview.

INSPECTOR COMMENTS

Since the Director of the Office of Security and Emergency Operations did not specifically concur or non-concur with the report recommendations, we believe it is critical that the Director's initial submission under the Department's Audit Report Tracking System (DARTS) clearly defines the rational for determining that any of the recommended actions are not appropriate or do not represent added value to the Site Safeguards and Security Planning Process. In addition, the Office of Security and Emergency Operations, in coordination with the National Nuclear Security Administration, should clearly define their plan for corrective actions in their initial submission under DARTS.

Appendix A

SCOPE AND METHODOLOGY

While reviewing the allegations discussed in this report, we evaluated:

- The reporting of the status of security at RFETS, TSD, and LANL through the SSSP process.
- The appropriateness of the actions taken by Department management to evaluate and resolve High Risk concerns identified by the contractor and the SSSP QA function.
- The appropriateness of the actions taken by Department management to evaluate and resolve other security weaknesses identified by the contractor.
- Changes to the SSSP process that eliminated the post-facto SSSP QA reviews.
- The issue of retaliation as it related to certain Department and contractor employees who were involved in the SSSP QA process.

As part of our review, we interviewed officials from the contractor organization, Los Alamos National Laboratory, Sandia National Laboratories, Pacific Northwest National Laboratory, and Department officials from the Office of Security and Emergency Operations, the Office of Safeguards and Security, the Office of Security Affairs, the Office of Defense Programs, the Office of Environmental Management, TSD, and the Albuquerque Operations Office.

In addition, we also reviewed documentation relating to the SSSP QA process, including: (1) SSSPs for TSD and LANL; (2) SSSP QA reports, including ALPHA Reports, Physical Security Systems Reports, an Integrated Report for TSD, and JTS Reports; (3) a Format and Content Guide for SSSPs; (4) Acceptance Criteria and Review Guide for SSSPs; (5) a Final Report of the Design Basis Threat Working Group and the SSSP Working Group; (6) the SSSP Rollout 2000 Workshop Report and the Tool Box Evaluation; (7) the Vulnerability Assessment Program Workshop Report; and (8) applicable Department of Energy Orders and Directives regarding security at Department sites.

This inspection was performed between January and June 2000. This inspection was conducted in accordance with the "Quality Standards for Inspection" issued by the President's Council on Integrity and Efficiency.

Appendix B

BACKGROUND

The SSSP describes safeguards and security programs and vulnerability and risk analysis at applicable sites. The SSSP is the primary instrument that the Department's Operations Office Managers use to certify to the Secretary of Energy the accuracy of risk and the measures used to assure that the public, employees, environment, and national assets are adequately protected. The SSSP is approved by Heads of Field Elements and concurred in by the cognizant Program Office and the Office of Security Affairs.

All SSSPs are to be certified annually as being current and valid, and are to be updated and approved at least once every five years unless a more frequent cycle is warranted. The Operations Office/Field Office Manager, in consultation with the Program Offices, Office of Independent Oversight and Performance Assurance, and the Office of Security Affairs, can direct that the SSSP be updated to reflect evolving threats and changes in a site's security posture.

In 1997, the Office of Nonproliferation and National Security began what they called "a rigorous and disciplined" QA process as part of the "review and verification" of the Department's SSSPs (referred to as the SSSP QA process). The Office of Safeguards and Security had found significant deficiencies in reporting "Risk," often due to the characterization of the Design Basis Threat and scenarios that did not stress the worst case. During this period, the Office of Safeguards and Security assigned the contractor the task of supporting the SSSP QA effort.

In an August 21, 1997, memorandum to various OSS Division Directors, the Director of OSS issued criteria and methodology that would be employed in the reviews of SSSPs. The purpose of this criteria and methodology was to address systemic SSSP verification issues that had arisen during prior reviews.

The SSSP QA process employed the use of three specific tools for review and verification of the Department's SSSPs. These included:

- Joint Tactical Simulation (JTS) - an interactive, entity-level conflict simulation modeling tool;
- Advanced Logic Protection Heuristic Analysis (ALPHA) - a vulnerability assessment tool; and,
- Physical Security Systems Reviews (PSSRs) - examinations, tests, and evaluations of the effectiveness of physical security systems.

In a November 4, 1998, memorandum to the OSS Acting Director, Field Operations Division, the OSS Director stated that he considered the reviews of SSSPs to be a "critical principle" function of OSS. The Director stated that the three "primary tools" used, ALPHA, JTS, and PSSRs, must be carefully integrated and appropriately documented for each SSSP. The Director also stated that it was expected that each of these tools would be used to evaluate all SSSPs unless timely equivalent information existed. The Director recognized that a "constructive tension condition" existed between the Safeguards and Security office responsible for the SSSP QA process and the Safeguards and Security office responsible for field assistance and expediting OSS concurrence with SSSP's. However, he stated that these checks and balances would result in a more effective safeguards and security program.

As part of its support role associated with the SSSP QA effort, the contractor reported that High Risk security conditions existed at the Rocky Flats Environmental Technology Site, and the Transportation Safeguards Division. Further, with regard to Los Alamos National Laboratory, the contractor concluded that "there is insufficient evidence to provide reasonable assurance that SNM [Special Nuclear Material] is protected to the standard required by the Department. . . . That is, SNM is not at low risk . . . ."

The contractor alleged that findings at these three sites were either ignored, or not acted upon in a timely manner. For example, it was alleged that the contractor identified High Risk at RFETS in March 1997, but no action was taken to address the High Risk condition until November 1999. Also, the contractor allegedly identified High Risk conditions involving TSD operations in the fall of 1998 that were never addressed, and that allegedly remain today. In reviewing the LANL SSSP in November 1999, the contractor allegedly found major problems with the ability of the protective force to deal with worst case scenarios that were never addressed, and also allegedly remain today. The contractor also alleged that the SSSP QA review process is currently being restructured, and that documents for this effort show a systematic pattern of "dumbing" down the SSSP process. The contractor explained that the SSSP QA process is being subverted so that SSSP development becomes a joint Field/Headquarters function with no independent review.

Appendix C

DEFINITIONS

Risk	Risk is defined as Low, Moderate, or High. Risk ratings are determined by evaluating the effectiveness of the protection system against events such as the threat of the theft of Special Nuclear Material (SNM), weapons, and weapons components. Department policy states that Low Risk Ratings are acceptable.
Design Basis Threat	The Design Basis Threat is a postulated threat used to design protective forces and security systems for the guarding of nuclear sites. The Design Basis Threat describes the most credible and serious potential adversaries, their tactics, numbers, and capabilities. The purpose of the Design Basis Threat is: (1) to provide a stable basis for security planning and budgeting that is predicated on a predetermined threat estimate which is not dependent on tactical intelligence, (2) to provide a baseline for DOE-wide protection standards for our most attractive nuclear assets, and (3) to provide a standard against which to evaluate the performance of protective forces and the effectiveness of installed security systems.
Verification and Validation	Verification is accomplished through the conduct of vulnerability assessments, use of modeling tools, evaluation of training and maintenance records, and table-top exercises of varying degrees of formality. Validation is a process where assumptions reached through assessments, modeling and evaluation activities are tested for validity, the predominant tool utilized being the performance test (ranging from tests of an individual's skills to a full scale force-on-force exercise).

IG Report No. DOE/IG-0482

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we nay any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

8

PERSONAL AND CONFIDENTIAL

January 5, 2000

General Eugene Habiger
Director, Office of Security & Emergency Operations, SO-1
U.S. Department of Energy
Washington, DC

Subject: Lying and Retaliation in the SO-20 Department.

It is with the utmost regret that I write this letter. There are two points I need to make. The two issues are: the first and most pressing issue is that of a number of people in the Department that are lying in the reporting of the actual status of security at our most important nuclear sites; the second issue concerns the illegal retaliation of these people against those trying to correct these security problems..

RETA Security, Inc. is part of the prime contract to provide support to Department SO-21 under contract DE-AC01-98NN50323. We have provided the key person services of Senior Engineer as well as Program Analyst since 1994. In that time we have provided services to both the Policy and Field Operations Branches. In 1997 we were assigned an additional task through the then NN-51 to support a QA effort through Richard Levernier for review of all 11 SSSPs for protection of Class A nuclear facilities. As part of that effort we worked with Mr. Levernier to develop a QA process that involved evaluation of the Parts I & II of the SSSP, the JTS simulations, and provide input for the on-site systems reviews.

In 1997, one of the first reviews we undertook was that of RFETS. In March of that year we documented high risk at this site. JTS simulations in April confirmed the assertion. Over the period of time since 1997 until November of this year literally no changes were made to improve the security at this site. We have found similar major problems at TSD in 1998, and LANL in 1999. There have been lesser problems at LLNL, SNLA, and Pantex. In all of these instances we have provided extensive analyses and documentation to support these findings. In all instances we were asked to make sure that the results were "bullet proof." We did.

In the spring of 1999 we were assigned to support the efforts of Mr. Peter Stockton on behalf of the Secretary of Energy. In that role we provided technical assistance in the preparation and documentation of nine issue papers that identified major security issues. Many of these issues are related to our efforts since 1997. We understand that you have been briefed on their content.

In the spring of this year we assembled over 90 official documents that tracked the history of problems at RFETS to include congressional requests for information, conditional concurrence by SO-20, OA inspections, etc. These documents show a systematic pattern of lying and misinterpretation of facts. For instance, in the fall of 1997 Joe Mahaley conditionally concurred with the 1997 SSSP if certain protective force actions were addressed within 120 days. None of the issues were addressed until November 1999. In 1998 OA ran a worst case force on force at

PERSONAL AND CONFIDENTIAL

RFETS which the site failed. The Inspection report said security was acceptable because three lesser tests were okay. The department has a policy for risk that is numerical value and defined adjectivally as either low, moderate or high. There is no designation as "acceptable." In the summer of 1999 Don Solich prepared a briefing paper for you that indicated no major problems at RFETS even though he was well briefed on the QA results.

In the fall of 1998 we did an extensive review of TSD. These findings were documented in January 1999 and briefed to Joe Mahaley and his staff through Johnson, Ford and Solich. At the initial briefing to Mahaley he said that he needed a day to think about results for TSD that clearly showed high risk. In the summer of that year, with nothing have been done about risk, Mahaley observed force on force testing at Ft. Hood. Based on this review he was prepared to offer SSSP concurrence. In the fall Stockton uncovered "cheating" at this test. To date Mahaley has done nothing to address the high risk. The TSD issue has been continually pointed out to Johnson, Ford, and Solich as a series of memos from Rich Levernier. We have documented over 15 briefings and correspondence on this issue.

In November of 1999 we did a review of LANL, TA-55 and found major problems with the ability of the protective force to deal with worst case scenarios. The results were documented to management to include, Johnson, Ford, and Solich. At the briefing, a HQ contractor asserted that the current SSSP did not in fact represents the current force profile and strength and that it had been greatly improved since seven days earlier. Therefore, the SSSP should be concurred with. This means that the SSSP did not have a VAR asserting any risk other than high. Never in my experience have I seen a situation were no documents supported risk, but that this line of management was prepared to recommend approval because "that is what the General wants."

Since the spring of this year I feel that we have become victims of a systematic retaliation and retribution effort by management in SO-20 to discredit our work and reduce our role in the QA effort needed for concurrence decisions by you. Joe Mahaley, Toby Johnson, Jim Ford, Don Solich, and Sam Calahan are currently engaged in obfuscating issues, and in some instances, lying to keep issues of high risk to national assets from being brought to your attention. Further, this systematic retaliation and retribution effort affects other personnel who were either part of the SSSP reviews, or assisted Peter Stockton. These persons include Marshall Combs, Larry Wilcher, Rich Levernier, Jack Pope, and other personnel from my company.

Currently there is a restructuring of the SSSP being undertaken. We have been systematically denied from participating in this effort by management. Requests by Rich Levernier for us to participate have been denied by Johnson, Ford, and Solich. When we have reviewed some of the documents from this and the DBT effort, we have found a systematic pattern of "dumbing" down the SSSP process. For example, the new SSSP proposes using 1989 values of consequence for loss of assets. The 1989 values were found to be flawed in 1993. They not only result in risk being less conservative by 13% or more, but they require no protection for Cat II SNM. Sam Calahan knows this, but has ignored the issue. Also the QA process is being completely subverted so that SSSP development becomes a joint Field/HQ function with no credible "hold" points for independent QA review functions. The DBT is examining the use of a truck bomb to

PERSONAL AND CONFIDENTIAL

cause radiological sabotage. This in spite of the fact that the NRC has expressly addressed the truck bomb and radiological sabotage. We know of at least one site that has vehicle barriers in the wrong location near a large inventory of Pu next to and up wind of a major metropolitan area.

The QA tools developed by Rich Levernier were attacked by Jim Ford. Ford asked for field comments about the QA process. Surprisingly the conclusion was that the QA process was not needed. The comments provided by the field whose SSSP were in question were basically sophomoric and self serving. The CTA model from course CTA-241 for advanced VA analysis was dropped by Sam Calahan in spite of class reviews that extolled its virtues. This model was an alternate to check VA results. With no checks and balances, the SSSP process is further "dumbed down."

After the initial Stockton support, he asked for our help on the consolidation issue. We have extensive experience in this area. Peter was told by Mahaley that RETA was too expensive and that our rate was $300 per hour. This is patently untrue. Our rates for my services are half of that, and others from our company are less than that. Not only that, but these rates have been accepted in contract negotiations with me designated as a key person. Ford and Johnson have also repeated this tale in public forums. I find this very unprofessional, besides being untrue. What this smacks of is denying Mr. Stockton resources he may need to accomplish his work in a timely and efficient manner. Further, it imputes our capabilities.

Since the spring of 1999 our use in support of QA efforts have had a steady decline. The rate of decline is symptomatic of all of the items identified above. The specter of retaliation and retribution is not one that we are corporately comfortable in dealing with. We work at the pleasure of any of our clients. When we have been ethically or professionally compromised we have left that client. We believe that the role that Secretary Richardson and you have signed up to to protect assets of societal importance is necessary, and therefore we have prepared this letter as a last resort. We believe this is not a "he said she said" issue, but based on documented evidence.

As you consider this letter I would invite you to contact what I consider impartial sources that will attest to our professional competence and ethical conduct. Two such persons are: Thomas Gradle, Director of Security, Chicago Operations, and Cliff Druit (BG, ret).

If you would like to meet with me personally, review the documents, or issues I would be pleased to make myself available at your convenience.

Sincerely yours,

Ronald E. Timm

Ronald E. Timm,
President
(630)257-3520

9

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-001

Extension

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	J. Cronin	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

Found significant deficiencies in reporting risk due to characterization of Design Basis Threat and scenarios that did not stress worst case. U

Finding Comment:

RECOMMENDATION: Establish policy on what actions are required to once High Risk and Moderate Risk are identified through the SSSP process, including the resolution of High Risk and Moderate Risk issues within specific timeframes; and the consideration of cmopensatory measures, formal acceptance of risk, and mitigation of risk through operational changes. U

Corrective Actions:

08/15/2001	Milestones: SOP to be developed to address roles and responsiblities regarding resolution of perceived differences in relative risk. Draft to be completed by 3/15/01. Finalize SOP - ECD 4/15/01. Identify roles and responsibilities for SO and NNSA (10/31/01) Implement SOP. After 6 months of SOP implementation, re-evaluate and modify SOP as appropriate.	U

Validation:

10

11

UNCLASSIFIED

U.S. DEPARTMENT OF ENERGY

Safeguards & Security Information Management System

40 Records found

Finding Data

Report Parameters

Classified	N	OSS Received Date Minimu	
Finding Status	O	OSS Received Date Maximum	
Facility Status	%	Topical Area Code	%
Lead Responsible Office	%	Subtopical Area Code	%
Importance Rating	%	Overall Topical Area Rating	%
Facility Code	%	Finding Responsible Office	%
Survey Type	IG	Finding Extensio	
Survey Date Minimum	01/01/1000	Finding Insert Date Minimum	01/01/1000
Survey Date Maximum	12/31/4000	Finding Insert Date Maximu	12/31/4000
Survey Report Number		Validation Date Minimum	
Corrective Action History	Y	Validation Date Maximum	

Order by

Highest Classification
Lead Responsible Office
Finding Status
Facility Code
Subtopical Area Code
Finding Number
Corrective Action

Maximum Classification on Report is

UNCLASSIFIED

FORMAT: LANDSCAPE

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 99NOV30-AL-13-IG-PM.1-001 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	08/01/2000	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	GP	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01FEB05-AL-13-SSPS	AL	SSPS	02/05/2001		PM	Marginal	PM.1
DOE/IG-0471	IG	IG	11/30/1999		PM		PM.1

Finding Description:

The LAAO security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs. U

Finding Comment:

RECOMMENDATION: Review and assess staffing levels for security personnel at LAAO, and ensure that the Area Office has adequate staff with the necessary technical expertise to carry out its security oversight responsibilities. U

Corrective Actions:

04/10/2000	INITIAL RESPONSE: LAAO security is understaffed. To alleviate this condition, LAAO maqnagement, together with AL management are currently working towards a process to assist in the oversight of LANL. AL/OSS provides matrix support to LAAO in all security functions. Efforts are in place to hire a security expert reporting to the LAAO Area Manager, to identify and resolve security issues at LANL. This individual will have the expertise to more effectively ensure security issues at LANL receive the necessary qualified attention from LAAO, AL, or HQ. Other staffing increase options are being considered. ECD: 12/15/2000.	U
07/31/2000	No change in status as reported 04/10/2000.	U
10/03/2000	No change in status or ECD as reported 04/10/2000.	U
12/18/2000	No change in status. ECD for reporting purposes: 03/15/2001.	U
04/05/2001	Two individuals with security responsibilities have been hired at LAAO; additional staffing is still under consideration. ECD for reporting purposes: 06/15/2001.	U
07/03/2001	No change in status as reported 04/05/2001. ECD for reporting purposes: 09/15/2001.	U

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 99NOV30-AL-13-IG-PM.1-001 **Extension**

10/30/2001	No change in status as reported 04/05/2001. ECD for reporting purposes: 12/15/2001.	U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 99NOV30-AL-13-IG-PM.7-002 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	08/01/2000	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	GP	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01FEB05-AL-13-SSPS	AL	SSPS	02/05/2001		PM	Marginal	PM.7
DOE/IG-0471	IG	IG	11/30/1999		PM		PM.7

Finding Description:

The AL survey team that conducted the 1999 survey at LANL was composed of some inspectors and support service personnel who had never been assigned to a survey team previously, and several who had not attended survey team training. U

Finding Comment:

RECOMMENDATION: Ensure that security survey team personnel possess the requisite expertise and skill necessary to perform the survey and that team members have sufficient experience in the topical areas being reviewed. U

Corrective Actions:

04/10/2000	INITIAL RESPONSE. Criteria are being established to determine an individual's qualfiications for inspection of each survey subtopic. In addition, a database is being developed to identify personnel who are potential survey team members and the subtopics they are qualified to inspect. The completion date is the second quarter of 2000.	U
07/31/2000	No change in status as reported on 04/10/2000.	U
10/03/2000	Data are still be compiled to complete the inspector/qualification database. ECD for reporting purposes: 03/15/2001.	U
12/18/2000	No change in status or ECD as reported 10/03/2000.	U
04/05/2001	No change in status as reported on 10/03/2000. ECD for reporting purposes: 06/15/2001.	U
07/03/2001	No change in status as reported 10/03/2000. ECD for reporting purposes: 09/15/2001.	U

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 99NOV30-AL-13-IG-PM.7-002 **Extension**

10/30/2001	No change in status as reported 10/03/2000. ECD for reporting purposes: 12/15/2001.	U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01SEP17-AL-13-IG-PPO.1-001 **Extension** DOE/IG-0523

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	10/05/2001	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	Albuquerque	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0523	AL	IG	09/17/2001		PPO	Does Not Apply	PPO.1

Finding Description:

Property coordinators duties are described throughout the Property Manual. U

Finding Comment:

RECOMMENDATION: The Manager, Albuquerque Operations Office require Sandia National Laboratory to consolidate all the duties and responsibilities of property coordinators in a single document. This document should specify that the duties include (a) completing all database identifier fields, such as descriptions, serial and model numbers and (b) updating and informing property management on the status of lost or stolen property. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01SEP17-AL-13-IG-PPO.1-002 **Extension** DOE/IG-0523

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	10/05/2001	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	Albuquerque	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0523	AL	IG	09/17/2001		PPO	Does Not Apply	PPO.1

Finding Description:

Sandia's Fixed Assets Database was not accurate. U

Finding Comment:

RECOMMENDATION: The Manager, Albuquerque Operations Office require Sandia National Laboratories to develop an action plan to ensure the database is accurate. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01SEP17-AL-13-IG-PPO.1-003 **Extension** DOE/IG-0523

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	10/05/2001	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	Albuquerque	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0523	AL	IG	09/17/2001		PPO	Does Not Apply	PPO.1

Finding Description:

The Manager, Albuquerque Operations Office require Sandia National Laboratories to develop an inventory methodology that includes: (1) the use of reverse samples--the tracing of property back to the database; (2) an objective methodology to validate all verification memos. The methodology should include validation of memos for off-site property on a rotating basis. U

Finding Comment:

None U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01SEP17-AL-13-IG-PPO.1-004 **Extension** DOE/IG-0523

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	Albuquerque, NM	Open	10/05/2001	AL

Facility Name Albuquerque Operations Office

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
13	A Level	Albuquerque	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0523	AL	IG	09/17/2001		PPO	Does Not Apply	PPO.1

Finding Description:

There were no performance measures that specifically addressed the accuracy of the Fixed Assets Database. U

Finding Comment:

RECOMMENDATION: The Manager, Albuquerque Operations Office require Sandia National Laboratories to develop performance measures to ensure the accuracy of the Fixed Assets Database. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00NOV20-HQ-272-IG-IS.2-001 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	01/12/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	T. Johnson	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		IS	Marginal	IS.2
DOE/IG-0488	HQ	IG	11/20/2000		IS	Does Not Apply	IS.2

Finding Description:

Ensure that the Department's policies and procedures for the transmittal of classified material are precisely executed. U

Finding Comment:

None U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00NOV20-HQ-272-IG-IS.2-002 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	01/12/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	T. Johnson	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		IS	Marginal	IS.2
DOE/IG-0488	HQ	IG	11/20/2000		IS	Does Not Apply	IS.2

Finding Description:

Ensure that officials of the Department and its contractors are held accountable for management failures that result in the improper transmittal of classified material. U

Finding Comment:

None U

Corrective Actions:

11/20/2000 The Deputy Secretary said that the Department will publish an award fee clause that will allow the Department to withhold award fee dollars for violations of security directives regarding the protection of classified information. He also said that a civil penalties regulation is being developed to impose civil penalties up to one hundred thousand dollars for the failure to protect classified information. The estimated publication date of the award fee clause and the civil penalties regulation is May 31, 2001. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00NOV20-HQ-272-IG-IS.2-003 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	01/12/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	T. Johnson	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		IS	Marginal	IS.2
DOE/IG-0488	HQ	IG	11/20/2000		IS	Does Not Apply	IS.2

Finding Description:

The Director, Office of Security and Emergency Operations ensures that officials of the Department and its contractors are knowledgeable of the Department's policies and procedures for the transmittal of classified material. U

Finding Comment:

None U

Corrective Actions:

11/20/2000 The Deputy Secretary stated that the Department will increase the level of security awareness throughout the Department. He said that special publications focusing on this issue are being developed and additional security education resources are being allocated. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00NOV20-HQ-272-IG-IS.2-004 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	01/12/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	T. Johnson	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		IS	Marginal	IS.2
DOE/IG-0488	HQ	IG	11/20/2000		IS	Does Not Apply	IS.2

Finding Description:

The Director, Office of Security and Emergency Operations establish a mechanism for Department contractors to obtain approval of, and to verify mailing addresses for transmittal of classified information U

Finding Comment:

None U

Corrective Actions:

11/20/2000 The Deputy Director said that, due to the significant volumes of sensitive information in SSIMS and the associated need-to-know concerns, efforts are underway in the Department to modify SSIMS to provide a read only capability of selected facility information. This will allow more organizations to access those portions of the system relative to their specific operation, without the threat of being able to modify or delete information contained in the system. U

11/27/2000 Effective November 27, 2000, the Safeguards and Security Information Management System was modified based on user's need to know. This resulted in the creation of seven new users access categories. The user access categories are Entire Database, Facility Data Only, Contract Data Only, Survey Data Only, Facility/Contracts, Facility/Survey, and Contracts/Survey. SSIMS contractor users, responsible for verifying classified mailing addresses, will be assigned Facility Data Only and will be restricted to the facility portion of the database. This will allow more organizations to access those portions of the system relative to their specific operation, without the threat of being able to query, modify or delete information contained on the system. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-272-IG-IS.4-001 **Extension** DOE/IG-0518

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	G. Podonsky	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

The Office of Independent Oversight and Performance Assurance could not always readily provide supporting documentation. U

Finding Comment:

RECOMMENDATION: The Director, Office of Independent Oversight and Performance Assurance develop and implement a structured approach to documenting and maintaining information to support each classified information system inspection report. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-272-IG-IS.4-002 **Extension** DOE/IG-0518

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	G. Podonsky	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

Policies and procedures to govern the conduct of cyber security inspections were incomplete at the time of the IG audit. U

Finding Comment:

RECOMMENDATION: The Director, Office of Independent Oversight and Performance Assurance adopt formal policies and procedures to govern classified system inspections. Such policies should specifically address topics such as the extent of coverage, areas of concentration, and overall review methodology. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-001 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	J. Cronin	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

Found significant deficiencies in reporting risk due to characterization of Design Basis Threat and scenarios that did not stress worst case. U

Finding Comment:

RECOMMENDATION: Establish policy on what actions are required to once High Risk and Moderate Risk are identified through the SSSP process, including the resolution of High Risk and Moderate Risk issues within specific timeframes; and the consideration of cmopensatory measures, formal acceptance of risk, and mitigation of risk through operational changes. U

Corrective Actions:

08/15/2001 Milestones: SOP to be developed to address roles and responsiblities regarding resolution of perceived differences in relative risk. Draft to be completed by 3/15/01. Finalize SOP - ECD 4/15/01. Identify roles and responsibilities for SO and NNSA (10/31/01) Implement SOP. After 6 months of SOP implementation, re-evaluate and modify SOP as appropriate. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-002

Extension

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	J. Cronin	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

The new SSSP process does not provide for the resolution of disputes. U

Finding Comment:

RECOMMENDATION: Ensure that a dispute resolution process is incorporated within the responsibilities of the Threat Assessment Quality Panel and the successor organization to the Security Management Board so that disagreements on the interpretation of the Design Basis Threat, adversary capabilities, and the assumptions that go into the identification, modeling, and testing of worst case scenarios are addressed at the highest level of management. U

Corrective Actions:

08/15/2001	SOP to be developed to address roles and responsibilities regarding resolution of perceived differences in relative risk. Draft to be completed by 3/15/01. Finalize SOP - ECD 4/15/01. Identify roles and responsibilities for SO and NNSA (10/31/01). Implement SOP. After 6 months of SOP implementation, re-evaluate and modify SOP as appropriate.	U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-003 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	AL, NNSA	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

The SSSP process did not ensure that validation of performance testing of response forces was based on worst case scenarios. U

Finding Comment:

RECOMMENDATION: Ensure that TSD validates the Special Response Force through the use of performance testing of the worst case scenarios. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-004

Extension

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	AL, NNSA	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

OSS oversight did not ensure performance assurance goals were met. U

Finding Comment:

Evaluate TSD's performance testing program and assure that all performance tests used to validate their SSSP's (a) are not encumbered by training priorities, (b) constitute legitimate force-on-force activities without coaching by instructors/controller, and (c) provide results that are conclusive in terms of measuring the ability of Special Agents to perform in response in an actual attack. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-005 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	Al, NNSA	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

OSS oversight did not ensure TSD validation of OSS comments. U

Finding Comment:

RECOMMENDATION: Ensure that TSD validates all other corrective actions that were identified on the "TSD Interim Disposition of NN Comments" matrix. U

Corrective Actions:

08/15/2001 There were 17 issues identified on the matrix. OTS developed a tracking process to address the issues. 12 of the 17 have been addressed through completion. The remaining 5 issues have been addressed and will be closed upon final completion of the OTS SSSP document. These 5 issues are requests for specific data to be included in the SSSP documentation. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-006 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Albuquerque Operations Office	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	AL, NNSA	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

OSS did not ensure selection of a suitable site for TSD exercises. U

Finding Comment:

RECOMMENDATION: Ensure that TSD identifies a site suitable for conducting force-on-force exercises for worst case scenarios. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00SEP28-HQ-272-IG-PM.2-007 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	GERMANTOWN, MD	Open	10/23/2000	HQ

Facility Name DOE HEADQUARTERS; GERMANTOWN BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
272	A Level	J. Cronin	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
	HQ	SSPS	05/04/2001		PM	Marginal	PM.2
DOE/IG-0482	HQ	IG	09/28/2000		PM		PM.2

Finding Description:

OSS protection program planning has not evaluated the "adversary what if? creep" which results from miscommunication and misapplication of the Design Basis Threat. U

Finding Comment:

RECOMMENDATION: Evaluate the concern that a "Super Adversary" is created by the application of the Design Basis Threat to worst case scenarios, and determine what action is needed to disseminate more prescriptive policy and adversary capabilities so that the threat and adversary attributes contained in the Design Basis Threat are clear, concise, and univerally understood by the Office of Security Affairs, Office of Independent Oversight and Performance Assurance, the Program Offices, and all affected field elements. U

Corrective Actions:

08/15/2001 Milestones: Through OSS involvement in SSSP development phase, ensure ACL is uniformly used to ensure that "threats and adversary attributes are clear, concise, and universally understood." Accomplished via OTS, LLNL, ANL-W, and Pantex SSSPs (6/30/01). Evaluation of SSSPs for uniform application of threats and adversary capabilities (ongoing). Finalize SSSP SOP. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-697-IG-IS.4-001 **Extension** DOE/IG-0519

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	CIO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0519	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

RECOMMENDATION: The Deputy Secretary of Energy provide the CIO with the authority necessary to monitor and evaluate the effectiveness of the Department's cyber security program. U

Finding Comment:

None U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-697-IG-IS.4-002 **Extension** DOE/IG0519

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	CIO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0519	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

The Department did not implement the structured assessment methodology developed by the CIO Council and NIST. U

Finding Comment:

RECOMMENDATION: The Deputy Secretary of Energy require the CIO to design and monitor the implementation of a structured, program-level cyber security assessment program based on the CIO Council Framework and NIST guidance documents. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-697-IG-IS.4-003 **Extension** DOE/IG-0519

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	CIO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0519	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

During evaluation observed problems with security program planning and management, to include problems with risk management, contingency planning, computer incident reporting, training management, configuration management and access control problems. U

Finding Comment:

RECOMMENDATION: The Deputy Secretary of Energy require each of the line organizations evaluated to design and implement a plan for correcting the cyber security weaknesses identified in this report. The plan should specifically address the requirement to prepare risk assessments. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-697-IG-IS.4-004 **Extension** DOE/IG-0519

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	CIO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0519	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

The Department lacked sufficient information to manage its network intrusion threat because of problems with incomplete or untimely reporting of cyber security incidents. U

Finding Comment:

RECOMMENDATION: To improve cyber security within the Department, recommend the Deputy Secretary of Energy finalize Departmental cyber security incident reporting requirements. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG30-HQ-697-IG-IS.4-005 **Extension** DOE/IG-0519

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	CIO, LPSO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0519	HQ	IG	08/30/2001		IS	Does Not Apply	IS.4

Finding Description:

The Department currently lacks specific, focused performance measures for monitoring and gauging the overall effectiveness of its unclassified cyber security program. U

Finding Comment:

RECOMMENDATION: To improve the cyber security within the Department, recommend that the Deputy Secretary of Energy ensure that the CIO, in conjunction with the Lead Program Secretarial Officers, complete efforts to establish specific, quantifiable cyber security performance measures and incorporate them into the Department's Annual Performance Plan. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01OCT26-HQ-697-IG-NMCA.2-001 **Extension** DOE/IG-0529

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	11/06/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	JM	Active	11/06/2001

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0529	HQ	IG	10/26/2001		NMCA	Does Not Apply	NMCA.2

Finding Description:

Inventory information from the Sealed Source Registry was not merged with NMMSS when the registry was discontinued in 1984. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations direct that inventory data from the defunct Sealed Source Registry be reviewed and updated in cooperation with NRC and, where appropriate, merged with NMMSS. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01OCT26-HQ-697-IG-NMCA.2-002 **Extension** DOE/IG-0529

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	11/06/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	JM	Active	11/06/2001

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0529	HQ	IG	10/26/2001		NMCA	Does Not Apply	NMCA.2

Finding Description:

The Department has never comprehensively confirmed NMMSS inventory balances by querying NRC and its licensees about the actual amount of nuclear material held by licensees. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations conduct a comprehensive confirmation of all balances of Government-owned nuclear materials held by domestic licensees and establish a schedule for future periodic confirmations that would include the full participation of the NRC. Resulting information should be reconciled with NMMSS data and necessary correcting entries made. Appropriate performance metrics should be established to control the process. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01OCT26-HQ-697-IG-NMCA.2-003 **Extension** DOE/IG-0529

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	11/06/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	JM	Active	11/06/2001

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0529	HQ	IG	10/26/2001		NMCA	Does Not Apply	NMCA.2

Finding Description:

NMMSS edit checks are not adequate to identify negative balances of Government-owned material or inventories associated with inactive or terminated licensees. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations enhance edit checks in NMMSS to immediately inform both governmental sponsors and other users that erroneous or anomalous data entries have occurred. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01OCT26-HQ-697-IG-NMCA.2-004 **Extension** DOE/IG-0529

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	11/06/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	JM	Active	11/06/2001

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0529	HQ	IG	10/26/2001		NMCA	Does Not Apply	NMCA.2

Finding Description:

Specific procedures for coordinating license terminations had not been developed. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations in cooperation with NRC, develop and implement enhanced procedures for the accounting of Government-owned materials. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01OCT26-HQ-697-IG-NMCA.2-005 **Extension** DOE/IG-0529

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	11/06/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	JM	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0529	HQ	IG	10/26/2001		NMCA	Does Not Apply	NMCA.2

Finding Description:

The Department has no procedures in place to confirm that materials are still needed or to incorporate such information into its disposition plans. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations develop and implement a process to periodically confirm the continuing need for Government-owned material at licensees and incorporate this information into Departmental material disposition plans. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01SEP11-HQ-697-IG-PM.2-001 **Extension** DOE/IG-0522

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	MD	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0522	HQ	IG	09/11/2001		PM	Does Not Apply	PM.2

Finding Description:

The Department's Office of Fissile Materials Disposition did not consider the FB Line or the TSF as alternatives for disposing of excess plutonium. U

Finding Comment:

RECOMMENDATION: The Acting Director, Office of Fissile Materials Disposition, analyze the FB line and the proposed TSF as alternatives to constructing the PIP. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG24-HQ-697-IG-PPO.3-001 **Extension** DOE/IG-0517

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	SO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0517	HQ	IG	08/24/2001		PPO	Does Not Apply	PPO.3

Finding Description:

Some firearms at the Headquarters facility were not on the SO inventory list or in the DOE Property System and others had serial numbers that did not exactly match the serial numbers on the list. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations, initiate action to ensure that firearms maintained by SO are appropriately controlled, accounted for, inventoried, and listed in the DOE Property System and in the SO inventory database. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG24-HQ-697-IG-PPO.3-002 **Extension** DOE/IG-0517

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	SO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0517	HQ	IG	08/24/2001		PPO	Does Not Apply	PPO.3

Finding Description:

NNSI officials did not inventory incoming excess firearms shipments within the time frames established by their internal procedures. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations, initiate action to ensure that NNSI officials fully implement their internal procedures regarding the receipt, inspection, inventory and storage of excess firearms received by NNSI. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG24-HQ-697-IG-PPO.3-003 **Extension** DOE/IG-0517

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	SO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0517	HQ	IG	08/24/2001		PPO	Does Not Apply	PPO.3

Finding Description:

NNSI officials did not, upon receipt, document the presence or integrity of tamper indicating devices or seals that were required to be on shipping containers of excess firearms sent to the facility. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations, initiate action to ensure that presence and integrity of TIDs or seals on boxes of excess firearms shipped to NNSI for storage are noted and documented upon receipt and appropriate action taken in the event of discrepancies. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG24-HQ-697-IG-PPO.3-004 **Extension** DOE/IG-517

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	SO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0517	HQ	IG	08/24/2001		PPO	Does Not Apply	PPO.3

Finding Description:

SO officials had not yet reconciled discrepancies identified during a 1998 inventory by the Office of Management and Administration (now Office of Management, Budget and Evaluation) officials of firearms stored at the facility. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security and Emergency Operations, initiate action to ensure that immediate steps are taken to resolve the discrepancies identified by the 1998 MA inventory, to include providing required documentation to MA. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 01AUG24-HQ-697-IG-PPO.3-005 **Extension** DOE/IG-0517

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	WASHINGTON, DC	Open	10/05/2001	HQ

Facility Name DOE HEADQUARTERS; FORRESTAL BUILDING

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
697	A Level	MA	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0517	HQ	IG	08/24/2001		PPO	Does Not Apply	PPO.3

Finding Description:

As a result of SO officials not reconciling discrepancies identified during a previous inventory by MA officials of firearms stored at the SO Headquarters facility, MA officials have not conducted an inventory of SO property for three years. U

Finding Comment:

RECOMMENDATION: The Director, Office of Management, Budget and Evaluation ensure that actions are initiated to quickly resolve discrepancies identified by Office of Management, Budget, and Evaluation inventories to assure that follow-on inventories can be performed in a timely manner. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00JUN29-RF-3772-IG-PM.2-001

Extension

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Rocky Flats Office	GOLDEN, CO	Open	10/23/2000	RF

Facility Name Kaiser-Hill Company, L.L.C

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
3772	A Level	RF Manager	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
DOE/IG-0475	RF	IG	06/29/2000		PM		PM.2

Finding Description:

Rocky Flats and its Contractor did not always account for and properly dispose of its weapon parts. U

Finding Comment:

RECOMMENDATION: The Manager, RFFO, establish controls to ensure that the Contractor: (1) Identifies and screens weapons parts prior to disposal; (2) Forwards weapons parts to sites where they are needed; (3) Controls accountable weapons parts; and (4) Documents the weapons parts shipped offsite. In addition, the Manager, RFFO, should clearly define the requirements to identify and segregate weapons parts when establishing performance measures involving the disposition of weapons parts. U

Corrective Actions:

09/15/2000 Final Proposed Management Decision for the Office of Inspector General Report IG-0475 transmitted to DOE Headquarters on 9/15/2000 via AMFPA:PA:REA:00-03563. Managment Decision indicates that the RFFO Manager concurs with both recommendations of the IG. In order to ensure and enforce the conduct specified in the previous direction, RFFO will re-direct KH by Contracting Office Technical Direction memorandum to continue to comply with the previous technical directions under the authority of the closure contract DE-AE34-00-RF01904. In addition, an assessment of the contractor's implementation of these technical directions will be conducted by RFFO in the third quarter of Fiscal Year 2001. U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00JUN01-SR-3803-IG-IS.2-001 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Headquarters	AIKEN, SC	Open	10/23/2000	SR

Facility Name WESTINGHOUSE SAVANNAH RIVER COMPANY, LLC

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
3803	B Level	Director, Office of Security & Emergency Operat	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01MAR29-SR-3803-SSPS	SR	SSPS	03/29/2001		IS	Satisfactory	IS.2
DOE/IG-0472	SR	IG	06/01/2000		IS		IS.2

Finding Description:

The Director, Office of Security and Emergency Operations should review existing policy and determine security vulnerability consequences resulting from the release of UCNI and security/privacy information. The results of the review should be incorporated into Departmental policy as appropriate. U

Finding Comment:

RECOMMENDATION: The Director, Office of Security Emergency Operations Office determine whether there are any possible security vulnerabilities resulting from the release of UCNI and security/privacy information. U

Corrective Actions:

08/15/2001 Reviewed and evaluated policy, including drafts. By definition - there are security vulnerabilities that result from the release of UCNI. MILESTONES: Review and modify policy as appropriate. The UCNI Order is being modified and will be placed in formal review (REVCOM) by 4/1/01. Publish revised policy by 8/1/01. The OUO Order was modified and is out for informal review (2/01) Submit OUO Order to REVCOM by 4/1/01. Publish revised policy by 5/31/01. Placed on hold due to Policy Review. OUO Order waiting on Trivelpiece review. ECD? U

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00JUN01-SR-3803-IG-IS.4-001 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Savannah River Operations Office	AIKEN, SC	Open	10/23/2000	SR

Facility Name WESTINGHOUSE SAVANNAH RIVER COMPANY, LLC

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
3803	B Level	Manager, SROO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01MAR29-SR-3803-SSPS	SR	SSPS	03/29/2001		IS	Satisfactory	IS.4
DOE/IG-0472	SR	IG	06/01/2000		IS		IS.4

Finding Description:

Westinghouse failed to comply with Departmental and site property management requirements by not properly preparing surplus computer equipment for disposal. U

Finding Comment:

RECOMMENDATION: Manager, Savannah River Operations Office require Westinghouse officials to ensure CSSO's or custodians inspect and certify all computer equipment for proper clearance prior to turning in the equipment for disposal. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00JUN01-SR-3803-IG-IS.4-002 **Extension**

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Savannah River Operations Office	AIKEN, SC	Open	10/23/2000	SR

Facility Name WESTINGHOUSE SAVANNAH RIVER COMPANY, LLC

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
3803	B Level	Manager, SROO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01MAR29-SR-3803-SSPS	SR	SSPS	03/29/2001		IS	Satisfactory	IS.4
DOE/IG-0472	SR	IG	06/01/2000		IS		IS.4

Finding Description:

Westinghouse did not clear stored information from all surplus computers and certify that the computers were sanitized prior to disposal as required by Section 109-43-307-53, title 41, Code of Regulations. U

Finding Comment:

RECOMMENDATION: Manager, Savannah River Operations Office require Westinghouse officials to ensure all computer equipment will be checked for certification to confirm that magnetic media and diskettes are properly cleared before being declared excess. U

Corrective Actions:

Validation:

U.S Department of Energy
Safeguards & Security Information Management System
Finding Data

Finding Number 00JUN01-SR-3803-IG-PM.1-001

Extension

Finding Responsible Office	Location	Finding Status	Insert Date	LRO
Savannah River Operations Office	AIKEN, SC	Open	10/23/2000	SR

Facility Name WESTINGHOUSE SAVANNAH RIVER COMPANY, LLC

Facility Code	Importance Rating	Analyst Name	Facility Status	Update Date
3803	B Level	Manager, SROO	Active	

Report Number	Surveying Office	Survey Type	Survey Date	OSS Received Date	Topical Area Code	Topical Area Rating	Subtopical Area
01MAR29-SR-3803-SSPS	SR	SSPS	03/29/2001		PM	Satisfactory	PM.1
DOE/IG-0472	SR	IG	06/01/2000		PM		PM.1

Finding Description:

Westinghouse violated the Department's requirements for disposing of high risk personal property. U

Finding Comment:

RECOMMENDATION: Evaluate the process used by Westinghouse to protect Privacy Act information which is maintained on behalf of the Department. U

Corrective Actions:

Validation:

12

Department of Energy
Germantown, MD 20874-1290

NOV 4 1998

MEMORANDUM FOR BROOKS E. TODD, ACTING DIRECTOR, NN-513

FROM: EDWARD J. MCCALLUM,
DIRECTOR, OFFICE OF SAFEGUARDS AND SECURITY

SUBJECT: SSSP REVIEWS

As you know, I consider our reviews of SSSP's to be a critical principal OSS function. The three primary tools that we use, ALPHA, JTS/JCATS and Physical Security Systems Reviews (PSSR's) must be carefully integrated and appropriately documented for each SSSP. It is expected that each of these three tools will be used to evaluate all SSSP's (this includes annual update submissions to confirm the absence of any changes to the baseline, resolution of prviously identified issues and progress on upgrades) unless timely equivalent information exists. When appropriate equivalent information exists and we plan to use it in lieu of our own analysis, I wish to be informed of that recommendation by NN-513.1. I would like to approve all recommendations to accept alternate analyses after they have been provided to our subject matter experts for review. Finally, when the SSSP quality assurance analyses are complete and fully integrated, please schedule the team leaders (ALPHA, JTS/JCATS, PSSR) to provide me a briefing.

I recognize that a constructive tension condition exists within NN-513, i.e. with NN-513.1 responsible for SSSP quality assurance and NN-513.2/.3 responsible for field assistance and expediting OSS concurrence with SSSP's. However, I am confident in your abilities to effectively manage and resolve the inherent problems associated with this "tension". These checks and balances result is a more effective DOE safeguards and security program which is our joint goal.

cc:
Richard J. Levernier, NN-513.1
Donald Solich, NN-513.2/.3

13

United States
Department of Energy

Monetary Award for Special Act or Service

Presented to

Richard J. Levernier

In recognition of your significant contributions in leading a team to review the Rocky Flats Site Safeguards and Security Plan. Your dedicated efforts and expertise have been instrumental in protecting the national safeguards and security interests of the United States.

Eugene E. Habiger, GENERAL, USAF (RETIRED)
Director
Office of Security
and Emergency Operations

February 2000

Printed with soy ink on recycled paper

DOE F 3450.4 (10-94)

14

DOE F 5635.3
(05-94)
All Other Editions Are Obsolete

U.S. DEPARTMENT OF ENERGY

CLASSIFIED DOCUMENT RECEIPT

OMB Control No
1910-1800
OMB Burden Disclosure
Statement on Reverse

TO

Mr. Dave Jones, SO-211
U.S. Department of Energy
P.O. Box 23865
Washington, DC 20026-3865

POSTAL NUMBER

DATE MAILED
Hand Carried 11/4/99

INSTRUCTIONS

1. Verify addressee's classified mailing address.
2. Describe document by subject or title and originator. See DOE 5635.1A for when this form is required.
3. Show classification and extra markings.
4. Forward original and duplicate to addressee.
5. Retain copy pending return of signed original by addressee.

FROM

Mr. Richard Levernier
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20878

DESCRIPTION OF DOCUMENT (Subject or title and originator)	IDENTIFICATION NUMBER	DATE OF DOCUMENT	CLASSIFICATION (Indicate whether or not RD, FRD or NSI)	COPY and SERIES	NUMBER of PAGES
1. Memorandum from Richardson to All Department and Contract Employees, Subject: Secretarial Policy Statement: Security Incidents & Violations		6/17/99	U		3
2. Memorandum from Levernier to McCallum, Subject: Transportation Safeguards Divsion (TSD)(U)		12/22/98	S		2
3. ALPHA Verification and Analysis Report of the Transportation Safeguards Division Draft Site Safeguards and Security Plan (U), Final Report		1/21/99	S		51
4. Joint Tactical Simulation (JTS) Study in Support of Office of Safeguards and Security Review of the Transportation Safeguards Divsion (TSD) Draft Site Safeguards and Security Plan (SSSP) (U)		1/21/99	S		27
5. Site Safeguards and Security Plan Physical Security Systems Report		3/1999	S		20
6. Integrated Verification Report on Security for the Transporation Safeguards Division		4/16/99	S		12
7. TSD Event Chronology		undated	U		1
8. Memorandum from Levernier to McCallum, Subject: Results of Draft Transportation Safeguards Division (TSD) Site Safeguards and Security Plan (SSSP) Review		4/19/99	S		7

I have received the document(s) listed above and assume responsibility for safeguarding in accordance with security regulations.

Signature of addressee or name of addressee and signature of recipient. _____ *Date* _____

Received for addressee by Karen Smith *Date* 11-4-99
(to be used only by mail rooms)

1. Return to Sender 2. Addressee's Copy 3. Pending Copy

Printed with soy ink on recycled paper

DOE F 5635.3
(05-94)
All Other Editions Are Obsolete

U.S. DEPARTMENT OF ENERGY

CLASSIFIED DOCUMENT RECEIPT

OMB Control No.
1910-1800
OMB Burden Disclosure
Statement on Reverse

TO

Mr. Dave Jones, SO-211
U.S. Department of Energy
P.O. Box 23865
Washington, DC 20026-3865

POSTAL NUMBER

DATE MAILED

INSTRUCTIONS

1. Verify addressee's classified mailing address.
2. Describe document by subject or title and originator. See DOE 5635.1A for when this form is required.
3. Show classification and extra markings.
4. Forward original and duplicate to addressee.
5. Retain copy pending return of signed original by addressee.

FROM

Mr. Richard Levernier
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20878

DESCRIPTION OF DOCUMENT (Subject or title and originator)	IDENTIFICATION NUMBER	DATE OF DOCUMENT	CLASSIFICATION (Indicate whether or not RD, FRD or NSI)	COPY and SERIES	NUMBER of PAGES
9. Memorandum from Levernier to Johnson, Subject: Transportation Safeguards Division (TSD) 1998 Site Safeguards and Security Plan (SSSP) with attachments		5/7/99	S		13
10. Memorandum from Johnson to Hafner, Subject: TSD Site Safeguards and Security Plan (SSSP)		6/30/99	S		6
11. Memorandum from Hafner to Johnson, Subject: Transportation Safeguards Division (TSD) Response to Verification/Validation Reports		7/2/99	U		1
12. Memorandum from Levernier to Johnson, Subject: Significant Transportation Safeguards Division (TSD) Security Concerns (U)		7/16/99	S		5

I have received the document(s) listed above and assume responsibility for safeguarding in accordance with security regulations.

Signature of addressee or name of addressee and signature of recipient. _____ *Date* _____

Received for addressee by Karen Swift *Date* 11-4-99

(to be used only by mail rooms)

1. Return to Sender 2. Addressee's Copy 3. Pending Copy

Printed with soy ink on recycled paper

15

DOE F 5634.1
(05-94)
All Other Editions Are Obsolete

U.S. DEPARTMENT OF ENERGY

OMB Control No.
1910-1800

SAFEGUARDS AND SECURITY SURVEY REPORT

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Resources Management Policy, Plans, and Oversight, Records Management Division, HR-422 - GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

1. Survey Type: ☐ Initial ☐ Periodic ☐ Special ☐ Termination		2. Report #
3. Facility Name:	4. A. Facility Code: B. RIS Code:	
5. Survey Date(s):	6. Findings: ☐ Yes ☐ No	7. Composite Rating:
8. Previous Survey Date(s):	9. Unresolved Findings: ☐ Yes ☐ No	10. Previous Rating:

11. Ratings:

A) PROGRAM MANAGEMENT

Program Management and Administration	____
Program Planning	____
Personnel Development and Training	____
Facility Approval and Registration of Activities	____
Foreign Ownership, Control, or Influence	____
Safeguards and Security Plans	____
Surveys and Self Assessment	____
Resolution of Findings	____
Incident Reporting and Management	____
OVERALL RATING	____

B) PROTECTION PROGRAM OPERATIONS

Physical Security	____
Security Systems	____
Protective Force	____
Security Badges, Credentials and Shields	____
Transportation Security	____
OVERALL RATING	____

C) INFORMATION SECURITY

Classification Guidance	____
Classified Matter Protection and Control	____
Special Access Programs and Intelligence Information	____
Classified Automated Information Systems Security	____
Technical Surveillance Countermeasures	____
Operations Security	____
Unclassified AISS (Optional)	____
Protected Distribution System (Optional)	____
Communications Security (COMSEC) (Optional)	____
OVERALL RATING	____

D) NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY

Basic Requirements	____
Material Accountability	____
Material Control	____
OVERALL RATING	____

E) PERSONNEL SECURITY

Access Authorization (Personnel Clearance)	____
Security Education Briefings and Awareness	____
Control of Visits	____
Unclassified Visits and Assignments by Foreign Nationals	____
Personnel Assurance Program	____
Personnel Security Assurance Program	____
OVERALL RATING	____

12. Surveying Office:

13. Report Prepared by:

Date:

14. Report Approved by:

Date:

15. Distribution:

Rate Each Item: S = SATISFACTORY M = MARGINAL U = UNSATISFACTORY DNA = DOES NOT APPLY

Printed with soy ink on recycled paper

16

DOE/IG-0471

INSPECTION REPORT

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF INSPECTIONS

SUMMARY REPORT ON INSPECTION OF ALLEGATIONS RELATING TO THE ALBUQUERQUE OPERATIONS OFFICE SECURITY SURVEY PROCESS AND THE SECURITY OPERATIONS' SELF-ASSESSMENTS AT LOS ALAMOS NATIONAL LABORATORY

MAY 2000

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.

Department of Energy

Washington, DC 20585

May 30, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (signed)
Inspector General

SUBJECT: INFORMATION: Summary Report on "Inspection of Allegations Relating to the Albuquerque Operations Office Security Survey Process and the Security Operations' Self-Assessments at Los Alamos National Laboratory"

BACKGROUND

The Office of Inspector General received allegations regarding the conduct of security reviews at the Department of Energy's (DOE) Los Alamos National Laboratory (LANL). Specifically, it was alleged that DOE Albuquerque Operations Office (Albuquerque) management changed the ratings of annual Security Surveys of LANL security operations after members of the Albuquerque Security Survey team completed the survey. It was also alleged that LANL Security Operations Division personnel were pressured by their managers to change or mitigate findings in LANL Self-Assessment reports.

RESULTS OF INSPECTION

Regarding the Albuquerque Security Surveys of LANL Security Operations, we found that:

- Albuquerque management changed ratings for the 1998 and 1999 surveys without providing a documented rationale for the changes;

- Albuquerque management did not fully address concerns about a compromise of force-on-force exercise during the 1998 Albuquerque Security Survey at LANL; and

- The 1997 and some 1998 Albuquerque Security Survey work papers were destroyed contrary to Albuquerque policy on the destruction of records. As a result, there was no complete record to show how ratings were developed by the survey teams.

Regarding the LANL Security Operations' Self-Assessments reports, we found that:

- Approximately 30 percent of the LANL Security Operations Division personnel interviewed, who had been involved in the conduct of self-assessments, believed they had been pressured to change or "mitigate" security self-assessments;

- Some security self-assessments required by LANL procedures were not being conducted; and

- DOE's Los Alamos Area Office security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs.

We concluded that the processes used to develop the Albuquerque security surveys of the LANL security operations and the LANL self-assessments were inadequate. As a result, there are legitimate concerns that the overall security condition at LANL, specifically for Fiscal Years 1998 and 1999, was not being accurately reported.

We provided management with a number of recommendations that, if implemented, would improve the effectiveness of Albuquerque security surveys and LANL self-assessments.

MANAGEMENT REACTION

Albuquerque management stated that the facts presented and the conclusions reached were accurate, and that the recommendations were appropriate. Albuquerque management stated that they would take corrective action.

Due to the concerns identified during our inspection, we recommended that the Department review these operations at other facilities. Specifically, we requested that the Director, Office of Security and Emergency Operations evaluate self-assessment programs at other DOE facilities to determine if they have been fully implemented and adequately represent security conditions. The Director agreed to this recommendation.

Attachment

cc: Deputy Secretary
Under Secretary
Acting Under Secretary for Nuclear Security/Administrator for Nuclear Security
Director, Office of Security and Emergency Operations
Manager, Albuquerque Operations Office

SUMMARY REPORT ON INSPECTION OF ALLEGATIONS RELATING TO THE ALBUQUERQUE OPERATIONS OFFICE SECURITY SURVEY PROCESS AND THE SECURITY OPERATIONS' SELF-ASSESSMENTS AT LOS ALAMOS NATIONAL LABORATORY

TABLE OF CONTENTS

Overview

Introduction and Objectives 1

Observations and Conclusions 1

Details of Findings

Changes to Security Survey Ratings 2

Management Rationale for Rating Changes 3

Compromise of Force-on-Force Exercise 3

Destruction of Records 4

LANL Self-Assessments 4

Los Alamos Area Office Oversight 6

Recommendations 7

Management Reaction and Inspector Comments 8

Appendices

A. Scope and Methodology 9

B. DOE Survey Requirements 10

C. 1998 Security Survey Rating Changes 12

D. 1999 Security Survey Rating Changes 13

Overview

Introduction and Objectives

The Office of the Inspector General received information from two complainants relating to security reviews at the Department of Energy's (DOE) Los Alamos National Laboratory (LANL). LANL is operated by the University of California under contract with DOE. One complainant alleged that managers of DOE's Albuquerque Operations Office (Albuquerque) Safeguards and Security Division, changed the ratings of periodic (annual) Security Surveys of LANL security operations after members of the Albuquerque Security Survey team completed the survey. Specifically, it was alleged that the Security Division managers upgraded survey ratings that were "Marginal" or "Unsatisfactory" as a result of "deals struck" between Albuquerque and LANL management officials. The second complainant alleged that LANL Security Operations Division personnel were pressured by their managers to change or mitigate self-assessment findings in LANL Self-Assessment reports. Both complainants alleged that the Albuquerque Security Survey reports at LANL and the LANL Self-Assessment reports did not clearly reflect the overall security conditions found by the survey field reviewers.

The objectives of our inspection were to determine: 1) if Albuquerque Security managers changed Albuquerque Security Survey ratings of LANL Security Operations; 2) if there was a basis for these changes; and, 3) if LANL Security Operations Division management had pressured its staff to alter self-assessment reports. This inspection did not include an evaluation of the overall security conditions at LANL.

During the course of this inspection, a number of individuals requested confidentiality. They indicated they feared retaliation for disclosing information to the Office of Inspector General (OIG).

Observations and Conclusions

We concluded that the processes used to develop the Albuquerque Security Surveys of the LANL Security Operations and the LANL Self-Assessments have raised legitimate concerns that the overall security condition at LANL was not being accurately reported.

Details of Findings

Details of Findings

In order to ensure compliance with DOE requirements,[1] the Albuquerque Safeguards and Security Division conducts annual security surveys of LANL Security Operations. The topical areas evaluated during these surveys include: Program Management, Protection Program Operations, Information Security, Nuclear Materials Control and Accountability, and Personnel Security. Each topical area also has several sub-topical areas. The Albuquerque Operations Office assigns ratings of "unsatisfactory," "marginal," or "satisfactory" based on conditions existing at the end of survey activities. A complete listing of the topical and sub-topical areas is provided at Appendix C.

Changes to Security Survey Ratings

Our inspection found that Albuquerque management changed ratings for the 1998 and 1999 Albuquerque Security Surveys of LANL Security Operations after the Survey Teams had assigned them. During the 1998 Albuquerque Security Survey at LANL, Albuquerque management upgraded several topic area survey ratings, and most importantly, the overall composite rating.[2] The OIG was told that had Albuquerque management not upgraded the topical and sub-topical ratings in the Nuclear Materials Control and Accountability topical area, and had management allowed the inclusion of a compromised force-on-force exercise, the overall composite LANL Security Survey rating would have been "Unsatisfactory."[3]

During the 1999 Albuquerque Security Survey at LANL, the overall composite rating was downgraded from "Satisfactory" to "Marginal" as were two sub-topical ratings and one topical rating.[4] The Survey Team initially rated LANL as "Satisfactory" based on the results of the 1999 Albuquerque Security Survey at LANL. However, during a final review, Albuquerque management determined that because the "23rd Annual Report to the President on the Status of Safeguards and Security at Domestic Nuclear Weapons Facilities," dated Jan 1997/Dec 1998, contained an issue concerning storage of classified parts, a "Satisfactory" rating

---

[1] The DOE requirements are specifically addressed at Appendix B.

[2] The 1998 rating changes are detailed at Appendix C. It should be noted that three of the seven ratings upgraded by Albuquerque management were the same as those ratings initially recommended by the Team Lead but subsequently downgraded by the "murder board."

[3] According to DOE Order 470.1, when a Survey has a composite rating of "Unsatisfactory" and the rating indicates a significant vulnerability, the Operations Office Manager shall coordinate with the cognizant Program Secretarial Officer within 24 hours to: 1) take action to shutdown/suspend operations of the facility or activity, pending remedial action, or 2) apprise the cognizant Secretarial Officer and the Office of Safeguards and Security of the rationale for continuing this critical operation and identify immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

[4] The 1999 rating changes are detailed at Appendix D. Team Lead ratings were not found for the 1999 survey.

would be the wrong message to send to the contractor. Therefore, the composite rating was downgraded from "Satisfactory" to "Marginal." Albuquerque management said that the composite ratings needed to closely reflect the results of other DOE reviews that had recently been conducted at LANL.

Management Rationale for Rating Changes

Although we found no evidence to support allegations of collusion or "deal making" between Albuquerque and LANL regarding the changes to the survey ratings, we did find that the survey reports did not contain any record of the rationale used by Albuquerque management for changing survey ratings. Albuquerque managers said that although Security Specialists conduct the surveys and propose recommended ratings for the sub-topic and topic areas, Albuquerque managers reserve "the right to take a look at what the survey team has developed" and decide what "message" should be sent to the contractor. Albuquerque management said that the rating process was "subjective" and that ratings remain "fluid" until a final report is issued. Contrary to the process identified in the Albuquerque Security Survey Procedural Guide, the Albuquerque managers said that they view it as a mistake to have the Security Specialists assign ratings because they do not have the overall LANL security program perspective prior to assigning final ratings and issuing the final security survey report. Further, in pursuing this matter, we found no other source which could provide the documented basis to support the Albuquerque management position concerning rating assignments or changes.

1999 Albuquerque Survey Team

The Albuquerque security survey team that conducted the 1999 Security Survey at LANL was composed of some inspectors and support service personnel who had never been assigned to a survey team previously and several who had not attended survey team training. Albuquerque management said that the 1999 Survey Team was short on staff because they had difficulty hiring qualified people to fill positions that had been vacated by retirements and other turnover. Two survey team members and two previous Survey Team Leads said they had questioned Albuquerque management about the appropriateness of the 1999 survey team's experience and the sufficiency of the number of inspectors staffed to conduct the 1999 survey.

Compromise of Force-on-Force Exercise[5]

The OIG also found that Albuquerque management did not fully assess concerns about a compromise of a force-on-force exercise during the 1998 Albuquerque Security Survey at LANL. The OIG

[5] A force-on-force exercise is conducted as a performance evaluation to assess the capability of the safeguards and security system to meet performance objectives in response to an outside group referred to as an Adversary Force.

found that Albuquerque management refused to allow the survey team to include a finding concerning a compromise of a force-on-force exercise in the survey report, and did so without adequately investigating the alleged compromise. A Security Force-on-Force Exercise Specialist told us there were major concerns raised regarding the Guard Force response, that the exercise had not gone well, and that the concerns had been appropriately raised to Albuquerque management. Albuquerque management said they had been made aware of the concerns, however, there was no evidence of "cheating" and that "the losers always complain that the winner cheated." A Security Specialist said that, had the compromise of the force-on-force exercise been included in the 1998 Albuquerque Security Survey report, the composite rating would have been "unsatisfactory." Instead, LANL was given a "marginal" rating.

Destruction of Records

During our inspection we noted that the 1997 and some 1998 Albuquerque Security Survey work papers were destroyed contrary to Albuquerque's policy on the destruction of records. The OIG also noted that some 1998 and 1999 work papers were either missing, not organized, or did not contain adequate summarization to support the ratings in the survey reports. As a result, there was no complete record to show how the survey teams developed the ratings.

LANL Self-Assessments

Since the inception of the LANL security self-assessment process[6] in 1996, LANL has had a history of not meeting all of its established self-assessment requirements. Specifically, the LANL Fiscal Years 1997 and 1998 Tier III Self-Assessment End-of-Year Reports indicate that some required Tier I and II self-assessments were not completed and that the process was not consistently implemented.[7] During our inspection, LANL officials confirmed weaknesses in the Tier I and Tier II self-assessment processes. The OIG found that in one LANL division, Tier I reviews were not being completed because the Tier I security responsibilities were assigned on a part-time basis and other responsibilities held a higher priority. In another LANL division, the OIG found that there had been no Tier II self-assessments completed since March 1998 because staffing was not adequate given other priority work.

[6] The LANL self-assessment process is described at Appendix B.
[7] At the time of our report, the LANL FY-99 Tier III Self-Assessment End-of-Year Report had not been issued.

In addition to finding that some self-assessments were not conducted, the OIG also found an instance where a self-assessment report was written without a self-assessment review being conducted. The OIG was provided a copy of a Tier II Self-Assessment Report that was generated in 1999 to support a Tier II review that was never performed. The OIG was told that this report, prepared at the direction of a LANL manager, was provided to an Albuquerque Security Survey Team to represent a completed Tier II review. The LANL manager who was identified as directing the preparation of the report denied having knowledge of any such report being prepared.

Pressure to Change Or Mitigate Issues

Regarding LANL Self-Assessments, the OIG found that 8 of the 28 LANL Security Operations Division personnel interviewed (approximately 30 percent) who had conducted self-assessments believed they had been pressured to change or "mitigate" security self-assessments. Several of these individuals said LANL management appeared to be more concerned about making LANL and the Security Operations Division "look good" than reporting the actual security condition at LANL. The OIG was informed of two instances where LANL management became so upset with issues[8] raised by the initially assigned reviewers, that management reassigned other reviewers who subsequently determined that there were no issues to be raised and that the organizations were satisfactory.

In addition, the OIG was provided information which showed that LANL management downgraded 40 issues and four concerns initially identified in a self-assessment draft report to six concerns and six observations which appeared in the final report. When interviewed, a LANL manager said that the reviewer had raised some issues that could not be validated, other issues that were unsupportable, and that there appeared to be a personality conflict between the reviewer and the organization being reviewed.[9]

A senior LANL manager indicated that, given the number of self-assessment findings identified since 1995, there was no concerted effort to avoid or mitigate findings.

[8] LANL has developed their own definition for issues, concerns and observations. Issues are deficiencies discovered during an internal self-assessment that require a corrective action plan. Concerns and observations are suggestions that may require improvement and may be mentioned in the text of a report, but they do not require a corrective action plan.

[9] It should be noted that the reviewer had conducted self-assessments in the same organization for three years prior to this review and had no difficulties in reporting issues developed during the prior self-assessments.

Los Alamos Area Office Oversight

The OIG determined that DOE's Los Alamos Area Office (LAAO) security staff was not performing all of the oversight responsibilities associated with the LANL Security Operations Division programs. Several DOE personnel told us that LAAO security was understaffed and did not have the technical expertise required to conduct all their oversight responsibilities. An Albuquerque manager confirmed that LAAO is understaffed and that the present staff has not had the necessary training to conduct the tasks required by their assignments. The manager told us there has been a reduction in full time equivalent positions at LAAO, and Albuquerque has not been able to replace staff that retire or leave for other positions. The Albuquerque manager said the two staff members that remain at LAAO's Office of Security have the responsibility for oversight but they do not have the technical expertise in all areas for which they are responsible. As a result, the manager said Albuquerque has taken responsibility for the security areas for which the LAAO staff does not have the technical expertise. It should be noted that our review did not independently evaluate the staffing levels and experience of the LAAO staff.

Energy's Office of Independent Oversight and Performance Assurance

The Department of Energy's Office of Independent Oversight and Performance Assurance reviewed LANL security operations during 1999 and issued a report on August 27, 1999, titled, "Independent Safeguards and Security Inspection of Los Alamos National Laboratory." The OIG is providing our findings to the Office of Independent Oversight and Performance Assurance for its consideration.

Recommendations

Recommendations

We recommend that the Manager, Albuquerque Operations Office:

1. Ensure that the supporting rationale for changing survey ratings after they have been assigned by the Survey Team is documented, and that the justification and the rationale for the factors responsible for the composite facility rating are included in the survey report.

2. Ensure that Security Survey Team Personnel possess the requisite expertise and skill necessary to perform the survey and that team members have sufficient experience in the topical areas being reviewed.

3. Update the Albuquerque Security Survey Procedural Guide to comply with the Albuquerque Records Information Destruction Schedule with regard to the destruction of all survey and inspection files.

4. Ensure that LANL's self-assessment program is fully implemented at all three-tier levels.

5. Review and assess staffing levels for security personnel at the Los Alamos Area Office, and ensure that the Area Office has adequate staff with the necessary technical expertise to carry out its security oversight responsibilities.

The OIG recommends the Director, Office of Security and Emergency Operations:

6. Evaluate self-assessment programs at other facilities to determine if these programs have been fully implemented and adequately represent the actual security conditions at the facilities.

Management Reaction and Inspector Comments

Management Reaction

In their response to the draft report, Albuquerque management stated that the facts presented and the conclusions reached were accurate, and that the recommendations were appropriate. Albuquerque management stated that they would take corrective action.

The Director, Office of Security and Emergency Operations agreed to evaluate self-assessment programs at DOE facilities, given the concerns identified during the inspection.

Inspector Comments

The actions planned and taken by the DOE Office of Security and Emergency Operations and the Albuquerque Operations Office were responsive to the recommendations.

Appendix A

Scope and Methodology

The OIG conducted this inspection at Los Alamos National Laboratory (LANL), Los Alamos Area Office (LAAO), and the Albuquerque Operations Office (Albuquerque) from April through November 1999. To accomplish our review objectives, the OIG:

- Reviewed DOE O 470.1, "Safeguards and Security Program," and DOE O 471.2A, "Information Security Program;"
- Reviewed the Albuquerque Security Survey Procedural Guide;
- Interviewed Albuquerque, LAAO, and LANL personnel;
- Reviewed documentation relating to security surveys and self-assessments;
- Reviewed the Albuquerque Management Review Division report titled "Manipulation of Security Survey Results" dated July 9, 1999;
- Reviewed the House Select Committee Report referred to as the "Cox Report" dated January 1999; and the President's Foreign Intelligence Advisory Board's report dated June 1999;
- Reviewed self-assessment reports issued by the LANL Security Operations Division and Security Survey reports issued by the Albuquerque Operations Office; and
- Reviewed the Office of Independent Oversight and Performance Assurance's Independent Safeguards and Security Inspection of LANL dated August 27, 1999.

This inspection involved a review of the Albuquerque Security Surveys of LANL Security Operations and LANL's Self-Assessment Program for Fiscal Years 1997, 1998, and 1999.

This inspection was conducted in accordance with "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Appendix B

DOE Survey Requirements

The Department has mandated a "Safeguards and Security Program" through the issuance of DOE Order 470.1, SAFEGUARDS AND SECURITY PROGRAM. The purpose of this order is to ensure appropriate levels of security protection consistent with DOE standards to prevent unacceptable, adverse impacts to national security.

DOE Order 470.1 establishes that the responsible Operations Office assign ratings of "unsatisfactory," "marginal," or "satisfactory" based on conditions existing at the end of survey activities; and that survey reports include a justification and rationale for the overall composite facility rating. The order specifically states that these ratings are not to be based upon future or planned corrective actions. Additionally, the order establishes that the survey team personnel who conduct the Security Surveys are to possess qualifications, experience, and training (basic survey and team leader training) sufficient to accomplish effective and thorough surveys.

Albuquerque Security Survey Requirements

To assist in Albuquerque security survey reviews, the Albuquerque Safeguards and Security Division developed a Security Survey Procedural Guide dated May 22, 1997, which identifies the responsibilities of the Survey Team Lead, the Assistant Survey Team Lead, and the survey team members during each phase of the survey. This Guide outlines the survey team process. Specifically, the guide states that the DOE Team Lead is to conduct a "murder board" during which Topic Team Leads[10] support rating rationale/justification and assign final ratings. Survey team members also provide comments and clarifications for ratings assigned. The finalized information is then given to the report coordinator for inclusion in the survey report.

Self-Assessment Requirements

DOE Order 470.1, Chapter X, SELF-ASSESSMENT PROGRAM, establishes the requirement for self-assessment programs at contractor facilities. It requires that self-assessment programs be conducted and documented for all cleared facilities and that the self-assessments be performed between the security surveys, which are conducted by the responsible Operations Office.

The LANL Safeguards and Security Self-Assessment Program is also mandated by the terms of the Department's contract with the University of California, contract modification No. W-7405-ENG-36. This contact modification requires that "... the University will conduct an ongoing self-assessment process including self-

[10] A "Topic Team Lead" is the individual assigned to head the team that reviews one of the five topic areas as identified in Appendix C.

assessments performed at the Laboratory as the principal means by which to evaluate compliance with the performance measures ... against which [the] University's overall performance of obligations under the contract will be determined."

The University of California, in compliance with contract requirements, has implemented a self-assessment program that is defined in a LANL Safeguards and Security Assurance Manual dated June 1996. This manual establishes a three tiered self-assessment process with a primary objective of ensuring the effective and efficient implementation of the LANL Safeguards and Security program.

The formalized safeguards and security self-assessment program includes a plan for each applicable topical and sub-topical area. The self-assessment process consists of a three-tier process. At Tier I, each LANL Division is required to conduct a self-assessment within the division. This is accomplished by the organizational safeguards and security officer, utilizing a checklist format, covering areas such as computer security, information security, property protection, and Nuclear Material Control and Accountability. At Tier II, each section within the LANL Security Division is required to conduct a self-assessment in their functional area(s). At Tier III, a LANL self-assessment is conducted by a team of Subject Matter Experts (SMEs) under the direction of LANL Security Division Program Integration Group.

Appendix C

1998 Security Survey Rating Changes[11]

Program Topic Areas:	Team Leader	Murder board	Final Report
Program Management			
Program Management and Administration	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Program Planning	Satisfactory	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Satisfactory	Satisfactory	Satisfactory
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory	Satisfactory
Safeguards and Security Plans	Unsatisfactory	Unsatisfactory	Unsatisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory	Satisfactory
Resolution of Findings	**Satisfactory**	**Marginal**	**Satisfactory**
Incident Reporting and Management	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protection Program Operations			
Physical Security	Marginal	Marginal	Marginal
Security Systems	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Protective Force	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Security Badges, Credentials and Shields	Satisfactory	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Information Security			
Classified Guidance	Satisfactory	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Unsatisfactory	Unsatisfactory	Unsatisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Marginal	Marginal	Marginal
Nuclear Materials Control and Accountability			
Basic Requirements	**Marginal**	**Unsatisfactory**	**Marginal**
Material Accounting	Unsatisfactory	Unsatisfactory	Unsatisfactory
Material Control	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
OVERALL RATING	**Unsatisfactory**	**Unsatisfactory**	**Marginal**
Personnel Security			
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory	Satisfactory
Security Education Briefings and Awareness	Satisfactory	Satisfactory	Satisfactory
Control of Visits	Satisfactory	Satisfactory	Satisfactory
Unclassified visits and Assign by Foreign Nationals	**Satisfactory**	**Marginal**	**Satisfactory**
Personnel Assurance Program	Satisfactory	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory	Satisfactory
1998 Composite Rating	**Unsatisfactory**	**Unsatisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

[11] There is no documentation for the 1999 Security Survey that provides a similar Team Leader rating breakdown.

Appendix D

1999 Security Survey Rating Changes

Program Areas:	Murder board	Final Report
Program Management		
Program Management and Administration	Satisfactory	Satisfactory
Program Planning	Satisfactory	Satisfactory
Personnel Development and Training	Satisfactory	Satisfactory
Facility Approval and Registration of Activities	Marginal	Marginal
Foreign Ownership, Control, or Influence	Satisfactory	Satisfactory
Safeguards and Security Plans	Satisfactory	Satisfactory
Surveys and Self Assessment	Satisfactory	Satisfactory
Resolution of Findings	Satisfactory	Satisfactory
Incident Reporting and Management	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Protection Program Operations		
Physical Security	Satisfactory	Satisfactory
Security Systems	Satisfactory	Satisfactory
Protective Force	Satisfactory	Satisfactory
Security Badges, Credentials and Shields	Satisfactory	Satisfactory
Transportation Security	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Information Security		
Classified Guidance	Satisfactory	Satisfactory
Classified Matter Protection and Control	**Satisfactory**	**Marginal**
Special Access Programs and Intelligence Information	Satisfactory	Satisfactory
Classified Automated Information Systems Security	Satisfactory	Satisfactory
Technical Surveillance Countermeasures	Satisfactory	Satisfactory
Operations Security	Satisfactory	Satisfactory
Unclassified AISS (Optional)	Satisfactory	Satisfactory
Protected Distribution System (Optional)	Satisfactory	Satisfactory
Communications Security (COMSEC) (Optional)	Satisfactory	Satisfactory
OVERALL RATING	**Satisfactory**	**Marginal**
Nuclear Materials Control and Accountability		
Basic Requirements	Satisfactory	Satisfactory
Material Accounting	Marginal	Marginal
Material Control	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
Personnel Security		
Access Authorization (Personnel Clearance)	Satisfactory	Satisfactory
Security Education Briefings and Awareness	**Satisfactory**	**Marginal**
Control of Visits	Satisfactory	Satisfactory
Unclassified Visits and Assignments by Foreign Nationals	Satisfactory	Satisfactory
Personnel Assurance Program	Satisfactory	Satisfactory
Personnel Security Assurance Program	Satisfactory	Satisfactory
OVERALL RATING	Satisfactory	Satisfactory
1999 Composite Rating	**Satisfactory**	**Marginal**

Items in **Bold** indicate changes in ratings.

IG Report No. DOE/IG-0471

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we nay any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

This page intentionally left blank.

17

Department of Energy
Germantown, MD 20874-1290

August 30, 1999

SO-20 let's discuss

A22

MEMORANDUM FOR: General Eugene E. Habiger, Director
Office of Security and Emergency Operations, SO-1

FROM: Barbara R. Stone, OA-10

SUBJECT: Recent Issues Regarding Vulnerability Analyses

During the last several years the Office of Safeguards and Security Evaluations has noted an accumulation of problems pertaining to the conduct of Vulnerability Analyses in support of Site Safeguards and Security Plans (SSSPs). In general, these problems pertain to the identification of adversary pathways and the representation of adversary tactical capabilities. The problems speak to a lack of consistency and rigor in the analytic processes that are used in support of the risk calculations that are central to the SSSP process. We believe that the time has come to address these problems on a Department-wide basis.

Our specific recommendations for resolving these problems, along with a more detailed supporting analysis, is presented in the attached position paper. If you would like to discuss these matters further, please contact me at 3-5895.

Barbara R. Stone

Barbara R. Stone, Director
Office of Safeguards and Security Evaluations
Office of Independent Oversight
and Performance Assurance

Attachment (OUO)

cc w/attachment:
G. Podonsky, OA-1

Printed with soy ink on recycled paper

Office of Independent Oversight and Performance Assurance: Recently Identified Concerns Relating to the Preparation of SSSP/VAs

Introduction – This paper discusses concerns that have been identified during recent inspections with respect to the preparation of Vulnerability Analyses (VAs) in support of Site Safeguards and Security Plans (SSSPs) at various DOE sites. It outlines the nature of these concerns and presents a proposed course of corrective action.

There are two broad categories of SSSP/VA related concerns that have emerged during inspections conducted by the Office of Safeguards and Security Evaluations in the last several years. First, the field has experienced repeated difficulties in obtaining timely approval of SSSPs. This issue has been the subject of much recent attention and is currently being addressed by the SSSP Working Group. It will not be discussed in this paper.

The second—and more serious—concern pertains to the actual content and quality of the VAs that support the current SSSPs. This issue, which calls into question the very foundation of the risk calculations used throughout the Department, has received little attention from safeguards and security managers. It is this concern that forms the subject of this paper. The specific issues are grouped under three headings: (1) Weaknesses in the Depiction of Adversary Pathways; (2) Weaknesses in the Representation of Adversary Tactical Capabilities; and (3) Assumptions Concerning the Need to Analyze Only 'Worst-Case' Pathways. The following sections describe these issues in greater detail and present a proposal for addressing them within the larger framework of creating a more effective VA process.

Weaknesses in the Depiction of Adversary Pathways

Most DOE facilities use the ASSESS analytic tool to identify potential adversary pathways. This is perfectly reasonable. Although the ASSESS tool has its inherent weaknesses, it remains the best currently available method for achieving an objective rating of potential pathways. It is certainly stronger than largely subjective methodologies such as Alpha, which is fundamentally little more than a means of organizing subject matter expert opinion. Unfortunately, some sites are not making the best use of the ASSESS tool to generate solid, defensible pathway analyses. There are three ways in which the use of ASSESS could be significantly improved.

Assigned Detection and/or Delay Values Do Not Accurately Represent Actual Capabilities. ASSESS builds upon a detailed representation of all of the security-related features at a site, including such things as the delay times associated with doors and walls and the effectiveness of intrusion detection and assessment systems. By calculating the relative contribution of each path element in detecting or delaying an adversary, ASSESS is capable of identifying the optimal pathways for an adversary. Obviously, the ability of ASSESS to perform this function depends upon the assignment of numerical values for each protection element that do not distort that element's relative effectiveness. But, despite the fact that there is both reasonable guidance and

Official Use Only
...ssified information which may be exempt from public ...sclosure under Freedom of Information Act (5 U.S.C. 522), ...emption number(s) ... Approval by the Department of ...nergy prior to release is required.
...eviewed by: ...
...ate: 5/27/99

a sufficient body of experience within DOE to support appropriate determination of such values, errors often occur. This appears to be partly a function of carelessness—building an accurate ASSESS facility file is laborious, time-consuming work that rarely receives the required amount of resource support. It also appears to be a function of simply adopting the default values contained in the program without doing the necessary analysis and/or performance testing necessary to justify either the defaults or a user-defined modification. During one recent inspection, a facility was found to have assigned a detection probability for a non-destructive vehicle search—an inherently difficult task—that was identical to the detection value assigned for the detection of individuals traversing a PIDAS with multiple, complementary intrusion detection sensors. Although this was patently absurd, neither the modelers nor subsequent reviewers had challenged the number.

ASSESS Analyses Are Not Kept Up-to-Date. As already emphasized, the preparation of an ASSESS analysis is both labor and time-intensive. Furthermore, since it requires a fairly high level of expertise, facilities have often resorted to outside technical experts to conduct (or, at least, to supplement) the ASSESS preparation effort. And then, at least at some facilities, the effort essentially freezes. During one recent inspection it was noted that the ASSESS-identified adversary pathways used to support the SSSP had been developed several years ago, using a facility configuration that did not reflect significant upgrades in intrusion detection systems. Faced with these upgrades, a real-life adversary would certainly have searched for other pathways, likely the same pathways that an updated ASSESS model would have identified.

ASSESS Insider Analyses Are Disregarded. In addition to calculating pathways for outside adversaries, ASSESS also can calculate probable insider and collusion path strategies. Although these analyses are difficult to complete, the results have generally proven valuable. Recently, however, less and less attention is being given to either updating existing ASSESS insider analyses or to conducting new ones when changes in facility operations indicate. This appears, largely, to be an unintended consequence of Department-wide reliance on PSAP to mitigate the insider threat. In other words, in spite of clear guidance to the contrary, the increasingly common assumption seems to be that "if we place a category of insiders into PSAP, then we don't have to analyze the threat that they represent."

All three of these problems can be related, at least in part, to the unwillingness of sites to make a sustained commitment to keeping VAs completely up-to-date. This, in turn, appears to be related to the perception that SSSPs have no useful purpose and that minimal compliance with the SSSP/VA requirement is all that should be demanded.

Weaknesses in the Representation of Adversary Tactical Capabilities

In the early part of this decade, the probable outcome of engagements between an adversary team and the protective force was usually calculated using the Neutralization module in ASSESS. Over the last five years, most DOE facilities have replaced this with more tactically representational models, first SEES and then JTS (the most recent iteration, JCATS, is just now becoming available). These models, in effect, constitute a kind of electronic performance test. Although they are not inexpensive to conduct, they are considerably less expensive, test for test, than corresponding force-on-force tactical performance tests. Thus, sites have increasingly relied upon these models as the primary element in developing the Probability of Neutralization

numbers that are essential to an overall calculation of protection system effectiveness. In effect, the risk numbers found in most SSSPs today rely very heavily upon the outcome of battles fought on computer screens, with limited numbers of force-on-force tests to supplement the computer-generated results. But neither JTS modeling nor force-on-force testing is effective if adversary capabilities are not adequately represented. Several problems in this area have recently been observed.

There Are Significant Errors in the Database Supporting the JTS Combat Simulation Model. While JTS is capable of providing useful indications of performance effectiveness, this capability depends upon the accuracy of the weapons and munitions performance data incorporated into the model's databases. JTS uses a complex set of databases to model tactical engagements in a near "real-world/real time" manner. The program compares for a given weapons/munitions versus target set a series of probabilities to include:

- The probability that an individual, armed with a particular weapon, would engage the target;
- The probability that, if the target is within the effective range of the weapon/munition, the target would be hit; and
- The probability that a single hit would kill or disable the target.

Within the JTS databases, there are two primary table that are used to support the latter two probabilities, namely Probability of Hit (Ph) and Probability of Kill (Pk). During recent reviews of JTS files used in the DOE community, this office has identified significant errors in these two tables. These errors will either over or under estimate the outcome of specific engagements, leading to questions regarding the reliability of the overall results. In addition to the identified errors, a significant number of readily available weapons and munition types are not included in the database.

Capabilities of Available Adversary Weapons Are Not Being Accurately Represented. In the last year this office has catalogued a long list of readily available adversary weapons and tools that are not being used appropriately by the adversaries depicted in current SSSP/VAs. Among these are tactical smoke, irritant gases, anti-personnel and anti-vehicle explosive devices ("stay-behinds"), grenades, armor-piercing small arms ammunition, and communications disruption devices, to name but the most obvious. It has become "customary" in DOE to limit the use of such weapons and tools, creating the potential for artificially high calculations of protective force effectiveness. This situation is equally common in both JTS calculations and in MILES-based force-on-force testing.

Adversary Tactics Are Poorly Thought-Out. Observed adversary tactics used during JTS simulations and validation and verification force-on-force tests are frequently crude, and often do not rise to the level expected of troops who have completed basic infantry training. During one recent inspection, it was noted that the adversaries depicted in the site's analysis succeeded in gaining control of a target location at the onset of their attack—and then hunkered down in tactically worthless positions that sacrificed the benefit of this initial advantage. Adversaries sometimes take little or no advantage from outside overwatch positions or from the use of

"stay-behinds" to isolate a target location or channel the protective force response. In both performance testing and simulations, this is likely the result of inadequate preparation. Personnel assigned to portray adversaries in modeling and performance testing are generally given only a few days to prepare tactical plans. A special problem with JTS simulations is that, generally, one computer operator is assigned to control the entire adversary team, while three (sometimes more) operators are employed to represent the protective force. This leads to situations where one adversary element is well managed in the simulation, while other elements are neglected and relatively ineffective.

The Shock Value of an Actual Attack is Undervalued. The only element of surprise in a JTS simulation or in a force-on-force test comes when an adversary comes up with some new tactical twist. The most fundamental real-world surprise—the fact that an attack is actually taking place—can never be adequately represented in such activities. Yet vulnerability analyses uniformly assume that, with no prior warning whatsoever, personnel who have spent years conducting routine patrols punctuated by the occasional MILES drill will respond with composure and complete efficiency when faced with an actual attack. This is compounded by the fact that many protective force personnel have never been in an actual combat situation and have never experienced the sudden shock of casualties among colleagues and friends. The adversary in the real world would have no such disadvantage. Having planned the attack and having chosen to carry it out, the adversary team members are, presumably, psychologically prepared to carry it out. And it is reasonable to assume that the members of an adversary team are already inured to bloodshed. Despite this, the typical analysis makes no effort to weight system effectiveness numbers to compensate for this problem.

Weaknesses such as these are partly a function of the structure of DOE security itself. We have a place for managers and personnel with a background in protecting assets, be it former military policemen or products of our own security forces. But we have recruited only a few personnel down through the years whose expertise is in *attacking* facilities. Thus, we tend to think like defenders, not like attackers, even when the task at hand is to realistically represent the capability of the terrorist. A second weakness is the lack of institutional resources dedicated to maintaining an up-to-date picture of adversary tactical and technical capabilities. Currently, no one in DOE outside of the Office of Safeguards and Security Evaluations appears to have a consistent interest in either cultivating the adversary mind-set or an understanding of adversary capabilities.

Assumptions Concerning the Need to Analyze Only 'Worst-Case' Pathways

The most recent format and content guidance for SSSPs indicates that the SSSP only needs to contain detailed descriptions of the 'worst-case' scenario results. This has led to the misconception that the only scenarios that require full-scale analysis are identified worst-case scenarios. Thus, some facilities come up with a set of potential high-risk scenarios, analyze them, develop near and long term mitigation to describe in the SSSP, and then conclude their analysis. This, however, does not square with stated DOE guidance, which required that all potential high and moderate risk scenarios be evaluated and documented, even if only the worst-case scenarios are explicitly discussed in the SSSP. Moreover, a site cannot even determine which scenarios are worst-case, unless all conceivable scenarios are at least considered. Here again, the problem seems to be pressure to do the compliant minimum, instead of applying the resources necessary to do the job right.

Recommended Actions:

The common issue in all of these concerns is the need for greater consistency and rigor in the conduct of VAs. This should be addressed at two levels:

1. Expectations for VA conduct in these areas should be clearly established.

2. Headquarters-level quality control should be rigorously exerted.

To accomplish these tasks, a committee should be formed to establish expectations regarding the issues discussed in this paper, particularly the representation of adversary characteristics. This committee should consist of representatives from those organizations with direct interest in the protection of SNM, including NN, DP, EM, and OA. This same committee, augmented by appropriately qualified technical specialists, should also be made responsible for conducting detailed quality review of all SSSP/VAs.

The combined result of these two activities should be to ensure that (1) the expectations communicated to vulnerability analysts reflect a consistent DOE-wide approach to conducting rigorous analyses and (2) appropriate quality standards are maintained. In this manner we can assure that all risk calculations are made on the same basis, enhancing the ability of senior Departmental managers to make complex-wide risk/benefit decisions.

In addition to these broader policy responses, the Department should also take action to ensure the reliability of its JTS analysis tool by procuring from the U.S. Army a certified database that includes representative weapons/munitions available to both DOE protective forces and potential adversaries. This certified database should be distributed to all sites currently using JTS (and also to sites that have adopted JCATS, the newest JTS variant). The Army Material Systems Analysis Agency (AMSAA) has, as one of its missions, responsibility for developing certified databases for Department of Defense models (such as JTS). The Office of Safeguards and Security Evaluations has already had preliminary discussions with AMSAA's director regarding the provision of such a database. While cost estimates are not yet available, the cost to DOE should be minimal, since the Army has already developed this information for its own use. The primary question is which DOE organization should take the lead in implementing this system-wide enhancement.

18

Department of Energy
Germantown, MD 20874-1290

MAR 28 2000

MEMORANDUM FOR JAMES L. FORD, ACTING DIRECTOR
FIELD OPERATIONS DIVISION

FROM: RICHARD J. LEVERNIER, PROGRAM MANAGER
ASSESSMENT AND INTEGRATION

SUBJECT: Deadly Force Training Deficiencies at Rocky Flats

The purpose of this memorandum is to describe a problem, with potentially serious consequences, that currently exists at Rocky Flats. Several recommendations to address this issue are also provided for management consideration. While validating the Rocky Flats (RF) Site Safeguards and Security Plan (SSSP) in October 1999, the HQ SSSP Assistance Team review of protective force performance test documentation disclosed an alarming trend concerning the inappropriate use of deadly force. During protective force performance tests of response to criticality alarm building evacuations, site reports noted, "...the response of the protective force, when their orders to halt were disregarded, was to fire indiscriminately into the crowd of evacuees." The same report also stated, "It is difficult to justify the wholesale killing of the building evacuees, when none among them - even the adversaries - had yet exhibited any behavior which offered a clear risk to either special nuclear material (SNM) or the life of any protective force member." The report also stated, "Subsequent performance testing conducted Saturday, February 28 (Scenario #2), also revealed similar issues involving the use of deadly force against building evacuees who demonstrated no immediate threat to either SNM nor security police officers (SPOs), but who simply disregarded SPO orders to "halt" while evacuating in response to a criticality alarm. This situation offers potential liability, is of concern, and deserves further inquiry." (Reference RF Protective Force Test Report April 1998). Additionally, the July 1998 DOE Office of Independent Oversight and Performance Assurance Report on RF cited problems in the use of deadly force during protective force performance test exercises.

In response to the HQ SSSP Assistance Team concerns on this matter, RF provided documentation that showed remedial training had been conducted concerning the use of deadly force. Additionally, RF representatives stated that subsequent performance tests would be carefully monitored and evaluated from a use of force perspective. This information appeared reasonable and sufficient to address the issue from a SSSP standpoint.

In March 2000, HQ participation in the RF protective force redeployment initiatives and subsequent performance testing again disclosed similar serious concerns regarding the inappropriate use of deadly force by the RF protective force. Two Multiple Integrated Laser Engagement System (MILES) enhanced exercises were observed where protective force members "killed" building evacuees, controllers wearing orange safety vests, and each other. During the

ALL-STATE LEGAL®

55

Printed with soy ink on recycled paper

Reference #1

critique conducted immediately after the exercise, protective force and other site management personnel failed to raise concerns related to the inappropriate use of deadly force. In fact, no critical observations were surfaced by management at the critique. Site analysis of these exercises is still ongoing.

Some of the exercise controllers and evaluators, with the primary responsibility for evaluating protective force performance, were not qualified to evaluate protective force members decisions concerning the use of deadly force. Administrative personnel, safety professionals, personnel security specialists, and others lacking a comprehensive understanding of the DOE Deadly Force Policy were utilized in these critical roles. Accordingly, the feedback concerning protective force performance, including the application of deadly force, was flawed.

As we all know, in the real world (versus MILES enhanced exercises) serious consequences are associated with the use of deadly force. Since we rely heavily on MILES enhanced exercises for protective force training and testing, we must ensure that appropriate serious consequences exist concerning the use of deadly force in these environments. In law enforcement training environments, the typical "penalty" for killing a "friendly" is failure of the test. At RF, there are currently no negative consequences for the inappropriate use of deadly force. In fact, if the adversaries are "killed" in the process, the result is actually a win from the sites current perspective. This situation is unacceptable and must be addressed immediately.

Recommend that HQ request RF and the cognizant Program Office to address this critical issue immediately. We must jointly ensure that the RF protective force fully understands the DOE Deadly Force Policy and applies it appropriately in training and testing environments. We must ensure that the remedial training is effective and validated with appropriate testing. Finally, we must document our actions and ensure this issue is monitored carefully in the future. Please let me know if you have any questions.

cc:
Toby Johnson, SO-21
Skip Bowser, SO-211.1
Larry Wilcher, SO-211
Don Solich, SO-212.3
Kelly Coady, SO-212.3

19

U.S. Department of Energy
Washington, D.C.

ORDER
DOE 5670.3
9-4-92

SUBJECT: COUNTERINTELLIGENCE PROGRAM

1. PURPOSE. To establish the policies, procedures, and specific responsibilities for the Department of Energy (DOE) Counterintelligence (CI) Program.

2. INQUIRIES. Inquiries concerning this Order should be directed to the Office of Counterintelligence, IN-20, U.S. Department of Energy, Washington, D.C. 20585, Telephone 202-586-7560.

3. APPLICATION TO CONTRACTS. The provisions of this Order apply to all covered contractors to the extent implemented under a contract or other agreement. A covered contractor is a seller of supplies or services involving access to and protection of unclassified sensitive information, proprietary information, classified information, nuclear materials, or other safeguards and security interests under a procurement contract or subcontract.

4. REFERENCES. See Attachment 1.

5. DEFINITIONS. See Attachment 2.

6. POLICY. DOE's policy is to develop a counterintelligence program in compliance with Executive Order 12333, "United States Intelligence Activities" of 12-4-81 and such Executive orders as may supersede it, whose purpose to deter and neutralize foreign industrial or intelligence activities in the United States directed at or involving DOE programs, facilities, technology, personnel, unclassified sensitive information; and classified matter.

7. CONCEPT OF OPERATIONS.

   a. Each Headquarters and field element of the CI program will be designed to counter site-specific intelligence threats directed against its personnel, information, activities, facilities, and technologies.

   b. At Headquarters, the CI program will be implemented by the Office

of Counterintelligence, IN-20.

c. In the DOE Field Offices, each Field Office Manager shall designate a Federal employee to serve as the Field Office CI Program Manager (CIPM). This program manager will have direct access to the Field Office Manager for sensitive CI activities and/or issues. The Counterintelligence Program Manager is authorized to conduct inquiries and administrative investigations including reviews of pertinent DOE information in the fulfillment of the CI mission. When an inquiry or administrative investigation provides reason to believe that there may be a basis for an espionage investigation, the matter will be immediately referred to the Federal Bureau of Investigation (FBI). This Order does not authorize any DOE or contractor employees to conduct espionage investigations or any other criminal investigations.

d. The Counterintelligence Program Manager will work with each DOE covered contractor to implement the CI program. Each DOE covered contractor, with the DOE concurrence and coordination will designate a Contractor Counterintelligence Officer (CCIO) to assist in the implementation of the DOE Field Office CI program. The Contractor Counterintelligence Officer has authority to conduct preliminary inquiries and administrative investigations as described by the Field Office Counterintelligence Program Manager to assist in the fulfillment of DOE's responsibilities. The Contractor Counterintelligence Officer will have direct access to the DOE's Field Office Counterintelligence Program Manager and senior contractor management, on a need-to-know basis, for sensitive CI activities and issues.

8. RESPONSIBILITIES AND AUTHORITIES.

a. Director of Intelligence (IN-1) shall:

(1) Provide overall management of the CI program.

(2) Authorize all intelligence and counterintelligence activities within DOE conducted by authorized agencies of the intelligence community involving DOE resources including but not limited to personnel, facilities, technology, or materials.

(3) Recommend and promulgate all Departmental CI policy.

b. Director of Counterintelligence (IN-20) shall:

(1) Develop and implement methods, techniques, standards, and procedures for Departmental CI activities in accordance with applicable laws, regulations, intelligence procedures, and Departmental policies.

(2) Provide oversight for implementation of CI policy and procedures.

(3) Familiarize DOE CI personnel, including IN-20, DOE Field Office Counterintelligence Program Managers and Contractor Counterintelligence Officers, and other DOE employees working

on CI, with the provisions of E.O. 12333 and other applicable policies and procedures.

(4) Establish a Headquarters (HQ) CI element to ensure compliance with applicable portions of this Counterintelligence Program Order.

(5) Support DOE Field Offices, in coordination with the responsible Program Secretarial Officer or Lead PSO, in the implementation of the Department's CI Program, and provide appropriate assistance in support of international treaty requirements and authorized intelligence community or law enforcement agency CI operations.

(6) Perform DOE national level liaison with authorized intelligence community or law enforcement agencies on CI matters. Review and approve all DOE CI field liaison with HQ elements of the intelligence community. This does not apply to activities of the Inspector General carried out pursuant to the Inspector General Act of 1978, as amended, 5 U.S.C. Appendix 3; Executive Order 12334; or other law, Executive order, Presidential directive, or regulation applicable to the Inspector General.

(7) Coordinate IN-1 approval for all CI activities and CI operations support requested by authorized officials of the intelligence community.

(8) Serve as the single DOE focal point for the CI program, represent DOE on national level CI committees, and coordinate CI interactions with other U.S. Government agencies.

(9) Manage the Departmental CI Analysis Program to advise DOE offices of the foreign intelligence threat. Conduct threat analysis, risk assessments, analytical studies, and identify assets, trends and patterns of foreign intelligence service activities directed against DOE.

(10) Implement the Department's CI Awareness Program. Ensure that the latest trends, patterns or threats of foreign intelligence service activities are incorporated in the Department's CI Awareness Program. Determine DOE's CI Awareness Program goals and coordinate with each DOE Field Office Counterintelligence Program Manager to ensure that CI awareness training objectives are met.

(11) Establish a CI briefing/debriefing program for foreign travel and contacts, and CI orientation briefings for new Federal and contractor employees.

(12) Monitor visits and assignments of foreign nationals to DOE facilities to assess relevant data pertaining to foreign intelligence service activities. Accomplish intelligence community indices checks (name traces) for all Departmental elements.

(13) Establish a format and reporting system for DOE Field Office

Counterintelligence Program Managers to transmit CI information to DOE's Office of Counterintelligence (IN-20).

(14) Based on indicators of the existence or presence of espionage, conduct counterintelligence inquiries and administrative investigations.

(15) Provide appropriate support to intelligence operations approved by IN-1.

(16) Advise Office of Security Affairs (SA-1) and the cognizant PSO of CI investigations or inquiries into matters which might have a potential impact on DOE safeguards and security interests.

(17) Establish and maintain liaison with SA-1 and PSO's to facilitate the exchange and discussion of information regarding CI and/or safeguards and security related activities which may fall within the purview of both offices.

(18) Approve and issue Federal credentials and shields to the designated CI personnel.

(19) Develop and implement a procedure to provide for independent oversight of the program as required by DOE 5630.12A.

c. Director of Security Affairs (SA-1) shall:

(1) Ensure policy is effected to support the Department's mission at both HQ and Field levels for coordination and exchange of information with IN-20.

(2) In accordance with applicable laws and regulations, establish policy and procedures for allowing access to all records maintained by the DOE complex to CI personnel at HQ and in the field when needed to perform their official duties.

(3) Ensure that any incidents or activities, involving a CI interest, identified within SA, especially within such programs as Technical Surveillance Countermeasures (TSCM), Operations Security (OPSEC), Computer (ADP) and Personnel Security, are properly coordinated with the DOE Office of Counterintelligence and the appropriate U.S. Government agencies.

(4) Perform DOE national level liaison with authorized U.S. Government agencies on Security Countermeasures (SCM) matters, to include but not limited to, TSCM, Physical Security, Personnel Security, OPSEC, and Unclassified and Classified Computer Security.

(5) Serve as the single DOE focal point for Security Countermeasures (SCM) programs, represent DOE on national level SCM committees, and coordinate SCM interaction with other U.S. Government agencies.

(6) Administer the program for the conduct of preliminary

internal investigations of unlawful disclosures of classified information as specified in DOE 5631.5.

(7) Advise the Office of Intelligence (IN-1) of security investigations or inquiries into matters having a potential impact on DOE CI matters.

d. Program Secretarial Officers and comparable senior officials (includes the Assistant Secretaries for Conservation and Renewable Energy (CE), Defense Programs (DP), Fossil Energy (FE), Nuclear Energy (NE), Environmental Restoration and Waste Management (EM), and the Directors of Energy Research, (ER), Civilian Radioactive Waste Management (RW), New Production Reactors (NP)), shall ensure implementation, by providing adequate financial and personnel resources, of an effective CI program at activities for which they exercise institutional oversight responsibilities.

e. Director of Naval Nuclear Propulsion Program (NE-60) shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 U.S.C. 7158, note)) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Propulsion Program, implement and oversee all policy pertaining to CI activities under the Director's cognizance.

f. Managers of DOE Field Offices shall:

(1) Designate a Federal employee to serve as the CI Program Manager who will be the responsible Federal employee for implementing the CI program for the DOE Field Office and managing and administering local CI programs. The Counterintelligence Program Manager will have direct access to the Field Office Manager.

(2) Assure the implementation of the CI Program and applicable portions of this Order at all facilities under their control, including covered contractor and subcontractor locations.

(3) Ensure the CIPM receives ongoing CI training and sufficient updates necessary to satisfy requirements of this Order.

(4) Assure that Safeguards and Security field elements provide access to records including security and personnel security records as necessary for the CIPM to perform official duties. Develop standards for the protection of intelligence information developed from such records or security interviews in accordance with the Privacy Act and other applicable rules and regulations.

(5) Assure access to all administrative records, including but not limited to computer, financial, personnel, and any other records necessary for the Field Office Counterintelligence Program Manager to perform official duties.

(6) Ensure that all Federal and contractor employees are aware of the requirement to report all contact with foreign nationals, and/or citizens of sensitive countries regarding sensitive

subjects, classified information, or any CI related incidents, to include perceived efforts to obtain sensitive or proprietary data or other such attempts to obtain inappropriate cooperation. Additionally, all contacts with citizens of sensitive countries should be reported.

(7) Support all intelligence and CI efforts of other authorized agencies with investigative or collection jurisdiction over intelligence and CI activities, with concurrence of IN-1.

(8) Provide appropriate administrative and logistical support to the Field Office Counterintelligence Program Manager to allow for the successful implementation and conduct of the Field Office CI program.

g. Field Office Counterintelligence Program Managers shall:

(1) Ensure the development and implementation of a CI Program for DOE Field Offices, contractors, and subcontractors consistent with the intent of the Departmental CI Program.

(2) Develop and implement a CI Awareness Program to meet CI program objectives in conjunction with the security education and awareness program.

(3) Perform liaison with authorized local intelligence community and law enforcement agencies on counterintelligence matters.

(4) Advise IN-20 of any specific CI educational requirements in conjunction with unique facility needs to ensure that specialized training curriculum may be tailored accordingly.

(5) Establish a system for limited CI incident examination, inquiries, resolutions, and/or referral to the appropriate Intelligence Community/law enforcement agency.

(6) Notify IN-20 within 24 hours of all incidents involving suspected or identified foreign intelligence activities and all incidents involving suspected or identified technical penetrations affecting persons or facilities under their jurisdiction.

(7) Coordinate with the Office of Safeguards and Security (SA-10) to provide CI information for the foreign travel and contacts briefing program. Provide CI information for safeguards and security orientation briefings for new Federal and contractor employees.

(8) Establish and conduct a program for foreign travel and contacts debriefings.

(9) Establish a system to assure prompt transmittal of current CI threat information to contractor CI program designee.

h. Heads of Headquarters Elements and Field Organizations shall designate an individual(s) to be responsible for bringing to the attention of the contracting officer each procurement falling

within the scope of this Directive. Unless another individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Request for Procurement").

i. Procurement Request Originators or such Other Individuals(s) (the individuals responsible for initiating a requirement on DOE F 4200.33) or such other individual(s) as designated by the cognizant head of headquarters element or field organization shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Directive, (2) requirements for flowdown of provisions of this Directive to any subcontract or sub-award, and (3) identification of the paragraphs or other portions of this Directive with which the awardee, or if different, a sub-awardee, is to comply.

j. Contracting Officers, based on advice received from the procurement request originator or other designated individual, shall apply applicable provisions of this Directive to awards falling within its scope. For awards, other than management and operating contracts, this shall be by incorporation or reference using explicit language in a contractual action, usually bilateral.

BY ORDER OF THE SECRETARY OF ENERGY:

DOLORES L. ROZZI
Director of Administration
and Human Resource Management

REFERENCES

1. Atomic Energy Act of 1954, which gives the Secretary of Energy the authority to protect against the disclosure of information that could adversely affect the health and safety of the public or the common defense and security of the United States.

2. Executive Order 12333, "U.S. Intelligence Activities," of 12-4-81, which sets forth the membership of the U.S. Intelligence Community and defines the duties, responsibilities, and general provisions for the conduct of intelligence/counterintelligence activities.

3. Executive Order 12334, "President's Intelligence Oversight Board," of 12-4-81, which sets forth requirements for the U.S. Intelligence Community reporting of intelligence activities.

4. National Security Decision Directive 44, "Organizing to Manage On-Site Verification of Nuclear Testing," of 7-90, which defines the duties and responsibilities of applicable agencies.

5. National Security Decision Directive 47, "Counterintelligence and Security Countermeasures," of 10-5-90, which establishes the U.S. counterintelligence goals for the 1990's.

6. National Security Decision Directive 197, "Reporting Hostile Contacts and Security Awareness," of 11-1-85, which establishes a requirement for each department or agency of the U.S. Government to establish formal awareness programs and procedures for reporting hostile contacts.

7. DOE 2320.1C, COOPERATION WITH THE OFFICE OF THE INSPECTOR GENERAL, of 5-18-92, which establishes Department of Energy policy for cooperation with the Office of Inspector General.

8. DOE 5630.12A, SAFEGUARDS AND SECURITY INSPECTION AND ASSESSMENT PROGRAM, of 6-23-92, which establishes an independent inspection and assessment program to determine the effectiveness of the Department's safeguards and security policies and procedures including their implementation across the Department.

9. DOE 5631.1B, SECURITY EDUCATION BRIEFING AND AWARENESS PROGRAM, of 12-31-91, which establishes policies, responsibilities, and requirements for the implementation of a security education program for the Department of Energy.

10. DOE 5631.5, VIOLATIONS OF LAWS, LOSSES, AND INCIDENTS OF SECURITY CONCERNS, of 2-12-88, which addresses investigative authorities within the Department of Energy for violations of law.

DEFINITIONS

1. COLLECTION.

   a. The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence.

   b. Obtaining information or intelligence information in any manner, including direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources.

   c. The act of employing instruments and/or equipment to obtain qualitative or quantitative data from the test or operations of foreign systems.

2. COUNTERINTELLIGENCE. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, communications, or documents and other matter security programs.

3. ESPIONAGE. Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation.

4. FACILITY. An educational institution, manufacturing plant, laboratory,

office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

5. HUMAN INTELLIGENCE (HUMINT). Intelligence information acquired by human sources through covert and overt collection techniques and open source data from foreign media.

6. INFORMATION. Unevaluated material of every description, at all levels of reliability, and from any source that may contain intelligence information.

7. INQUIRY. The collection and examination of information to include records review and interviews to assess indicators of espionage.

8. INVESTIGATION. A comprehensive examination of facts or other pertinent information conducted by an authorized agency.

9. INTELLIGENCE. The product resulting from the collection, collation, evaluation, analysis, integration, and interpretation of all collected information.

10. INTELLIGENCE ACTIVITY. A generic term used to encompass any or all of the efforts and endeavors undertaken by intelligence organizations, including activities pursuant to collection, analysis, production, dissemination, and covert or clandestine activities. When used in the context of Executive Order 12333, the term intelligence activity means all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333.

11. INTELLIGENCE COMMUNITY AND AGENCIES WITHIN THE INTELLIGENCE COMMUNITY. A generic term defined in E.O. 12333 which refers to the following agencies or organizations:

    a. The Central Intelligence Agency (CIA);

    b. The National Security Agency (NSA);

    c. The Defense Intelligence Agency (DIA);

    d. The offices within the Department of Defense for the collection of specialized foreign intelligence through reconnaissance programs;

    e. The Bureau of Intelligence and Research of the Department of State;

    f. The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy;

    g. The staff elements of the Director of Central Intelligence.

12. SECURITY COUNTERMEASURES. Defensive security programs and activities that seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material.

<>

This site sponsored by the Office of Management & Administration of the US Department of Energy.

Operated by Innovative Web Applications, Inc. and

Powered by

Additional Comments Submitted by Richard Levernier for
Whistleblower Disclosure OSC File No. DI-02-0572

1. Letter to Special Counsel Scott Bloch, December 7, 2005

2. **Letter to Catherine A. McMullen, December 19, 2003**

3. GAO Report, "NUCLEAR SECURITY: NNSA Needs to Better Manage Its Safeguards and Security Program," GAO-03-471, May 2003.

4. U.S. DOE OIG, Audit Report on "Management of the Department's Protective Forces," DOE/IG-0602, June 2003.

5. GAO Testimony, NUCLEAR SECURITY: DOE Faces Security Challenges in the Post September 11, 2001, Environment," GAO 03-896-TNI, June 24, 2003.

6. **Letter to Catherine A. McMullen, February 10, 2004**

7. U.S. DOE OIG, Inspection Report on "Protective Force Performance Test Improprieties," DOE/IG-0636, January 2004.

8. **Letter to Catherine A. McMullen, August 26, 2005**

9. U.S. DOE OIG, "Inspection Report on Reporting of Security Incidents at the Lawrence Livermore National Laboratory," DOE/IG-0625, November 2003.

10. U.S. DOE OIG, Special Report on "Management Challenges at the Department of Energy," DOE/IG-0626, November 2003.

11. U.S. DOE OIG, Audit Report on "The Department's Basic Protective Force Training Program," DOE/IG-0641, March 2004.

12. U.S. DOE OIG, Special Report on "Management Challenges at the Department of Energy," DOE/IG-0667, November 2004.

13. U.S. DOE OIG, Inspection Report on "Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory," DOE/IG-0677, February 2005.

14. U.S. DOE OIG, Inspection Report on "Security Access Controls at the Y-12 National Security Complex," DOE/IG-0691, June 2005.

15. U.S. DOE OIG, Inspection Report on "Protective Force Training at the Department of Energy's Oak Ridge Reservation," DOE/IG-0694, June 2005.

16. **Email to Catherine A. McMullen and Tracy Biggs, September 7, 2005.**

17. "NNSA Security, An Independent Review," conducted by Richard W. Mies, Admiral USN (Retired), et al., May 2005.

18. Supplemental analysis: Side-by-side comparison of Mies Report and DOE rebuttal