



Department of Energy

Washington, DC 20585

March 4, 2005

Catherine McMullen
Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington, D.C. 20036-4505

Re: OSC File No. DI-02-0572

Dear Ms. McMullen:

Enclosed please find a letter dated May 29, 2003 from former Secretary of Energy Spencer Abraham to The Special Counsel with attached OSC File No. DI-02-0572. Both the letter and document have been redacted per your request in preparation for their addition to your FOIA Public Reading Room.

The Department of Energy would appreciate notice prior to these documents being placed in the Reading Room. If you have any questions, please feel free to contact me at (202) 586-6724.

Sincerely,

A handwritten signature in black ink, appearing to read "Isiah Smith, Jr.", with a large, stylized flourish at the end.

Isiah Smith, Jr.
Deputy Assistant General Counsel
for Administrative Litigation and Information Law

Enclosure



~~OFFICIAL USE ONLY~~



The Secretary of Energy
Washington, DC 20585

May 29, 2003

The Honorable Elaine Kaplan
The Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

Re: OSC File No. DI-02-0572

Dear Madam Special Counsel:

In response to your request to the Secretary of Energy of October 25, 2002, the Department of Energy (DOE) investigated the concerns and allegations presented to the U.S. Office of Special Counsel (OSC), File No. DI-02-0572. During our review, the claimant provided additional information intended to clarify the concerns and allegations presented to the OSC File No. DI-02-0572.

Based on a detailed review of both the correspondence transmitted from your office and additional information provided by the claimant, I have concluded that the allegations are unfounded, based on information that is dated, and do not constitute a substantial and specific danger to public safety and health. A detailed report is attached, which addresses each allegation.

The DOE is confident that all of its class "A" nuclear facilities and its Office of Secure Transportation are well equipped, trained, and prepared to protect the interest of national security. Enclosed is the DOE's paragraph-by-paragraph response to the concerns presented in the U.S. Office of Special Counsel File No. DI-02-0572.

The Department of Energy's Office of Independent Oversight and Performance Assurance conducts routine independent assessments of the Department's class "A" nuclear facilities and the Office of Secure Transportation and has

~~OFFICIAL USE ONLY~~
~~Contains Classification of Sensitive Information~~
~~Department of Energy Approval Required~~
~~opposed to Public Release~~

DOES NOT CONTAIN
OFFICIAL USE ONLY INFORMATION
Name/Org.: Michael L. Gates, NNSA Service Center Date: 02/08/2005

Printed on recycled paper

~~OFFICIAL USE ONLY~~

~~OFFICIAL USE ONLY~~

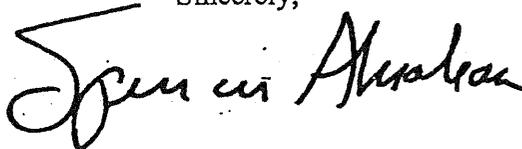
2

independently verified the effectiveness of the protection. The Office of Independent Oversight and Performance Assurance reports directly to me and is completely independent of the National Nuclear Security Administration and other DOE line organizations.

The additional information provided by the claimant identified a significant number of policy issues and a legal concern. The policy issues have been provided to the Office of Security and a working group is being established to address those issues. The legal concern has been provided to the Office of General Counsel, Office of General Law for appropriate action.

In the event you require any additional information or desire a briefing on these allegations, please do not hesitate to call me or have your staff contact Mr. Greg Rudy, Chief, Defense Nuclear Security, National Nuclear Security Administration, at (202) 586-7349.

Sincerely,

A handwritten signature in black ink that reads "Spencer Abraham". The signature is written in a cursive, flowing style.

Spencer Abraham

Enclosure

~~OFFICIAL USE ONLY~~

Investigation into Allegations
Referred to the Department of Energy
By the Office of Special Counsel

OSC File No. DI-02-0572

May 2003

DELETED VERSION

U.S. Department of Energy Declassification Review	
1 st Review Date: 02/08/2005 Authority: <input type="checkbox"/> AOC <input type="checkbox"/> DC <input checked="" type="checkbox"/> ADD Name: Michael L. Gates	Determination (Circle Number (s)) 1. Classification retained. 2. Classification change to: _____ 3. Contains No DOE Classified Info. 4. Coordinate with: _____ 5. Classification cancelled. 6. Classified Info. Bracketed. <input checked="" type="checkbox"/> Other (Specify): Does not contain OOU
2 nd Review Date: 02/09/2005 Authority: ADD Name: Charles L. Trujillo	

EXECUTIVE SUMMARY

This report responds on specific allegations made to the U.S. Office of Special Counsel regarding the security of the nuclear weapons complex. These allegations were referred to the Department of Energy (DOE) for investigation by letter from the Office of Special Counsel. The claimant stated that the information was obtained during employment with the DOE from March 1995 to August 2000. These allegations were identified as being based on personal observation during that period of time.

Some of the issues identified by the claimant existed during the 1995 to 2000 time period. However, many of the issues have been addressed multiple times by personnel from organizations both internal and external to the Department of Energy. Others are issues where there is a difference of opinion on how to implement an effective security program. In general, the allegations do not accurately represent the Department of Energy's current safeguards and security posture. The Department of Energy'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 National Nuclear Security Administration 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 Department of Energy, 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. The claimant would not be aware of the changes that have occurred in the last two years since he no longer has access to classified information nor a need-to-know for the information.

ALLEGATIONS

This report responds to specific allegations made to the U.S. Office of Special Counsel regarding the security of the nuclear weapons complex. These allegations were referred to the DOE for investigation by letter from the Office of Special Counsel. The claimant stated that the information was obtained during employment with the DOE from March 1995 to August 2000. These allegations were identified as based on personal observation during that period of time. During the course of the review of the allegations, a meeting was held with the claimant. Prior to that meeting the claimant provided an additional document. Based on the meeting and a review of the document, the claimant was requested to provide additional information on specific issues raised in the document. This additional information provided more detail that is addressed in this report. In addition the claimant identified a significant number of policy issues and a legal concern that were forwarded to the relevant organizations within the Department of Energy for appropriate action.

The allegations that were made deal with the safeguards and security protection provided to Class "A" facilities. Class "A" facilities are generally identified as those facilities that have Category I quantities of Special Nuclear Material. In general these are facilities that are engaged in work for the Department of Energy nuclear weapons complex. This complex is responsible for the design, development, construction, maintenance, repair and disposal of nuclear weapons for the United States. This mission is accomplished at a number of facilities.

The focus of most of the allegations is on the physical security for the Special Nuclear Material at facilities in the nuclear weapons complex. The security at these facilities is defined in DOE Orders and Regulations and implemented through a formal process that defines the specific protection levels to be provided. The allegations deal with both the implementation of physical security, as well as its oversight.

OVERVIEW

In order to put the allegations into proper perspective it is necessary to describe the process that is used to develop and implement the security posture of the nuclear weapons complex.

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.

The Design Basis Threat (DBT) document describes the spectrum of threats that must be protected against at DOE sites. The spectrum of threats ranges from terrorists to disgruntled employees. It identifies the attributes of each of the adversaries and their

motivations. In addition, the DBT identifies the type of attack that must be considered at DOE sites. This includes the potential for theft of materials or chemical, biological and radiological attacks as well as sabotage of DOE facilities.

VULNERABILITY ASSESSMENT

In order to be able to meet the Design Basis Threat, the DOE has a process that incorporates analysis, implementation, reviews and testing to assure the site can protect against the defined adversary. This process begins with a Vulnerability Assessment. A Vulnerability Assessment identifies those facilities and materials that contain the target material (Special Nuclear Material). The Vulnerability Assessment also includes the protection strategy required in order to define the level of protection for the facility. The Vulnerability Assessment uses a number of tools to identify the required level of protection. These tools have become progressively more sophisticated as time has passed. When this process was initially developed in the DOE in the early 1980's, some basic computer tools were developed that identified specific site pathways that an adversary would take to attack a site. A timeline for the attack was developed. An analyst would then evaluate additional detection or delay mechanisms that would allow the response forces to intercept the adversary. This simplistic modeling allowed the first look at the protection of a site.

COMPUTER MODELING CAPABILITY

Computer modeling has been used since the beginning of development of the Vulnerability Assessment process. Initially the models were fairly simple as described above. Over time, the capability for computer simulation of protection strategies has improved. The computer simulations used today allow individual protective force members to sit in front of computer screens with other individuals in front of other computer screens and simulate an intrusion at a specific site.

DELETED

This is a first generation three-dimensional modeling software. DOE is evaluating improved computer simulations that will use some of the commercially available software. These efforts include working with state-of-the-art computer simulation software companies.

The computer capability is used not only in the Vulnerability Assessment process, but also used in the continuing training of the security forces. Protective force personnel can begin to understand command and control of protective forces and can also see the impact of individual actions. DOE is continuing to evaluate other methods of using the computer simulations to improve the overall protective force strategy and tactics, as well as improve the training for security force personnel.

FORCE-ON-FORCE TESTING (MILES)

One of the tools that addresses real life situations for the protective force is the use of force-on-force testing. This testing is part of the Vulnerability Assessment process as well as the training of the security force. This testing allows security members to actually stand post and protect their site against 'real' adversaries. This process involved using the Multiple Integrated Laser Engagement System (MILES). This equipment uses existing weapons and replaces the bullets with laser beams. Individuals wear harnesses with sensors and when a laser strikes the sensor it informs the wearer that the beam has hit them. This system is similar to the current "laser tag" that is commercially available; however, it is designed for use with existing real weapons. An exercise involves pre-staging a protective force with laser equipment, an adversary force and a separate security force that has real weapons. A formal process involving controllers and evaluators is established to ensure the test is conducted following formal guidelines. This process allows simulation of actual tactics and evaluation of various protection strategies. It is typical that a large number of exercises are run when a site is first establishing its protection strategy. This allows refinement of both the tactics and numbers of response personnel to identify an optimum protection level for a site.

The MILES equipment has gone through a number of versions. All of the versions provide the basic principle of replacing bullets with lasers. As time has passed, improvements have been made to the equipment. The majority of these changes have been to add additional weapons to the MILES arsenal. Some of the latest technology changes have included additional reporting capabilities and the ability to determine which weapons had caused simulated damage to which adversary. Most major DOE sites have purchased their own MILES equipment in the past to allow them to conduct numerous exercises on sites whenever deemed appropriate. The equipment they use is typically dependent on the site needs and the version of the MILES equipment is based on the level of use of the equipment. Additionally, the NNSA is evaluating the potential costs and benefits of a large purchase of the latest generation of MILES equipment. This approach was discontinued in the past due to the difficulties in making the system meet all the needs of the field. Instead, sites purchased their own equipment in order to have maximum flexibility. If a decision is made to purchase this equipment, it will have to be budgeted and a system established for allocation of equipment. Additional information on MILES can be found at www.stricom.army.mil/PRODUCTS/MILES/.

The NNSA desires all protective personnel to participate in these exercises at least once per year. In addition, there is a need for exercises 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 exercises each year.

DELETED

ITERATIVE SITE ANALYSIS

A tool that has been developed in the last two years is the Iterative Site Analysis (ISA). This assessment tool was developed to allow facilities to take an in-depth, subjective look at the total threat spectrum. The ISA is a series of tabletop exercises where an adversary force provides their plan of attack against a selected facility on a site. The adversary force is made up of individuals who have significant experience as adversaries.

There are no limitations placed on the adversary other than they must be able to demonstrate that the actions they propose can be accomplished. This is normally based on the adversaries' experience and is reviewed by an independent team as part of the exercise. These current and former military personnel have had operating experience outside of the continental United States. While they have never been at the DOE site before, they are tasked with gathering information on the site just prior to the tabletop exercises. The exercise involves using the adversaries' attack plan and then seeing if the plan will meet the goals. This process is repeated with a variety of levels of adversaries and with different targets. When completed, it provides an overview of the protection level the site is providing. It also identifies potential improvements that can be made to address any specific issues that were identified in the exercise.

While this tool is useful, it is still a tabletop exercise and relies on professional judgment for the results of specific events. In order to provide additional information, the computer simulations and force-on-force exercises can be conducted to address specific issues.

SITE SAFEGUARDS AND SECURITY PLAN (SSSP)

The Vulnerability Assessment process is used to provide information for the formal protection strategy of the DOE sites. The formal documentation for the protection is put into the Site Safeguards and Security Plan (SSSP). This document identifies the protection level provided to the sites and the risks that are accepted. If there is a funding requirement to meet the protection levels, it is identified along with the projected funding availability. The document is developed by the site and coordinated with the appropriate federal personnel. This includes coordination with the local federal officials, who are responsible for formal risk acceptance. In addition, the document is coordinated with the headquarters personnel responsible for oversight of the implementation and the safeguards and security policy. The requirements for the SSSP are included in DOE Orders.

The SSSP documents the approved protection strategy. This strategy addresses the security requirements from the DOE Orders, Manuals and Notices. The SSSP meets a number of goals. Its main purpose is to document the protection approach. However, another part of the SSSP is to identify any areas where the site has determined it is appropriate to accept identified risks. This is an important part of the risk management

approach to security that is used in the DOE. The document also is designed to allow sites to identify future actions that will be taken based on future funding. The SSSP thus addresses both the current and the future protection levels of a site. Since this document summarizes the site efforts to meet the DOE Orders, Manuals and Notices, it is a very useful document for inspection teams to use to evaluate site performance. In addition, the SSSP can be compared against the DOE Orders to identify potential changes that may be needed in the DOE Orders. Attachment I contains a listing of the requirements for the DOE SSSP.

The specific allegations referred for investigation in OSC File No. DI-02-0572 were organized into four categories. These are:

- The alleged failure of the DOE class "A" facilities to employ explosive detection equipment as required by DOE Order,
- The alleged deficiencies in DOE's force-on-force performance tests at its nuclear facilities,
- The alleged deficiencies in DOE Safeguards and Security Programs, and
- The alleged security risks at the Los Alamos National Laboratory.

As identified earlier, this report responds to specific allegations made to the U.S. Office of Special Counsel. The following addresses the specific allegations on an individual basis. It is noted that part of the information provided alleges vulnerability with the Department of Energy's Office of Transportation Safeguards, now known as the Office of Secure Transportation. These allegations were provided by the claimant as part of a 39-page document. This document was provided during the process of gathering additional information to evaluate the original allegations. The 39-page document addresses many of the original concerns identified to the Office of Special Counsel as well as identifying new concerns. It is noted that many of the concerns identified in this 39-page document dealing with the Office of Secure Transportation were identical to those identified in the August 9, 2002, memorandum from the Honorable Condoleezza Rice, National Security Advisor, to the Department of Energy Secretary Spencer Abraham. This current request from the U.S. Office of Special Counsel and the previous request dealing with the Office of Secure Transportation bear the same OSC file number. The following sections address the specific allegations in the original request, as well as those related items that were provided in the 39-page document provided during the investigation of the allegations:

Lack of Explosives Detection Equipment

Allegation 1: The claimant stated that DOE's class "A" nuclear research facilities and laboratories are required by DOE Order 470.1 to use explosive detection equipment at certain points of entry. According to the informant, as of August 2000, none of the facilities were in compliance with this requirement.

The DOE Manual for Protection and Control of Safeguards and Security Interests, DOE M 5632.1C1, establishes the requirements for screening at points of entry to Protected

Areas and to Material Access Areas. The claimant stated that, in the absence of the requisite detection equipment, DOE is relying on compensatory security measures such as visual inspection for controlling available explosives detection equipment and that DOE is disregarding the security requirements it put in place to safeguard the inventory of Special Nuclear Material contained at its class "A" facilities.

Response 1: The DOE sites are not disregarding the DOE requirements for explosive detection. The requirement is to provide detection of explosives, not to require explosive detection equipment. This policy allows the use of explosive detecting animals (dogs) as well as use of screening techniques to detect explosives. The reason for this is an understanding of the various types of explosives that currently exist and the limitations that exist with the current generation of explosive detection equipment. The policy also takes into consideration that some of the DOE sites have explosives on site and this greatly reduces the practicality of commercially available explosive detectors.

While the DOE policy allows flexibility in the detection of explosives, the DOE also is taking steps to conduct research on new explosive detection equipment that would make the equipment more useful and detect other materials. DOE is also continuously reviewing new explosive detection equipment that is on the commercial market to identify any potential improvements that can be made to this aspect of security.

The DOE has been concerned over the potential use of explosives to aid an adversary in attacking DOE sites since the early 1980's. The Design Basis Threat has in the past and continues to identify the use of explosives by the adversary in attacking a DOE site. The Vulnerability Assessments and testing procedures used by the DOE include the use of explosives against targets at each site. Each DOE site has been required to formally identify how they address this concern in their SSSP. The detection of the potential introduction of explosives through the normal access locations is considered part of the protection strategy required for each DOE site that possesses Category I quantities of special nuclear material.

The DOE sites are required to be able to detect all types of explosives. Due to lack of commercial equipment developed for detecting a range of explosives, the DOE sites use other techniques including: x-ray equipment for packages, metal detectors for the containers for explosives, and individual searches of packages or personnel based on identified concerns. Since these methods address all types of explosives, additional explosive detection equipment is not needed, is expensive, and could lead to a false sense of security.

In addition to the difficulties of detecting various types of explosives, some sites have explosives on-site as part of their normal mission. Since the site personnel handle explosives on-site as a part of their job, the high rate of false alarms makes use of explosive detectors inappropriate at those sites. These sites must, therefore, rely on the use of x-ray equipment, metal detectors, and searches of packages and personnel.

The DOE approach to explosive detection is, and has been, consistent with the approach used within all of government (to include airports, military facilities and other facilities with high levels of security). The DOE laboratories and facilities have been, and continue to be, at the forefront in development of new detection equipment. DOE will implement these solutions when they are both cost-effective and meet the needs of the DOE sites. DOE also will continue to work with other federal agencies, such as the Federal Aviation Administration, to identify, evaluate, and test both government and commercial explosive detection equipment.

Alleged Deficiencies in DOE's Force-on-Force Performance Tests

Allegation 2: 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

DELETED

However, 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.

Response 2: The DOE sites routinely conduct performance tests of a wide variety of scenarios. These include a limited number of 'sabotage' scenarios. The purpose of the force-on-force test is to validate the protection strategies defined in the Site Safeguards and Security Plan and implemented at the site. They also keep the protective force current in responses that are close to real life. In many cases, theft of Special Nuclear Material is the highest potential concern at a site and many of the other scenarios are identified as threats of lower concern. The protection for these lower level threats is addressed by the protection provided by the theft scenarios. Thus, the claimant is correct in the observation that the DOE focuses on theft scenarios in the overwhelming majority of its performance tests. However, this is consistent with maintaining a high level of protection at the DOE sites.

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 for 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.

DELETED

Interim policies have been issued within the DOE that refocused attention on this issue. In addition, the upcoming DOE Design Basis Threat will provide additional specific guidance on this issue. In the meantime, the DOE sites have increased their efforts in this arena. As discussed above, new strategies and additional training have been implemented. 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.

The Office of Independent Oversight and Performance Assurance typically includes radiological sabotage and recapture/recovery scenarios in its performance testing at sites that have these requirements. This testing is conducted to help determine if the sites can protect against the radiological sabotage threat and have the capabilities to conduct recapture/recovery operations.

Allegation 3: *The claimant also alleges that DOE uses obsolete equipment in its performance tests.*

DELETED

MILES allows participants in force-on-force exercises to fire infrared "bullets" from the same weapons they would use in combat. It replicates the range and effectiveness of actual weapons systems approximating the adversary's capabilities. In addition, MILES identifies casualties and records the exercises so the performance of the personnel can be replayed and analyzed. This feature allows the force-on-force teams to evaluate the protective force's performance as well as the losses suffered.

Significant improvements have been made to MILES. According to the information from the informant, the system is in its fourth generation.

DELETED

DELETED

The claimant states that

DOE's continued use of this equipment produces inaccurate reports regarding protective force readiness and ability to defend DOE's nuclear assets.

Response 3:

DELETED

MILES is a tool to assist in validating tactics and keeping personnel at a state of readiness based on participating in simulated real-life exercises. The version of MILES that is used is dependent on the purpose it is supporting.

DELETED

The issue the claimant appears to be raising deals with detailed evaluation of exercises. The recent generations of MILES equipment includes the ability to record which weapons fired which shots. The normal exercises have sufficient numbers of personnel included in monitoring the actions. **DELETED**

Thus, sites can meet all of their needs using equipment that they currently possess. When that equipment is replaced due to life cycle needs, they will be replaced with the latest generation equipment. At the current time, three of the major DOE sites have upgraded to the fourth-generation equipment. Additional upgrades will take place in the future.

The fourth-generation equipment can be useful in the formal testing process used by the Office of Independent Oversight and Performance Assurance. Since this is a short time-frame exercise where the tests cannot be easily re-run, being able to analyze the exercise after the fact is useful.

DELETED

As noted in the discussion on MILES equipment, NNSA is evaluating the potential costs and benefits of a large purchase of the latest generation of MILES equipment. If a decision is made to purchase this equipment, it will have to be budgeted and a system established for allocation of equipment to meet the needs of the DOE sites.

DELETED

Allegation 4: The claimant alleges that DOE does not keep accurate records of protective force performance in these force-on-force exercises. For example, DOE does not keep records of losses sustained by the protective force, errors made by the protective force, fratricide by members of the protective force, or other violations of DOE's Deadly Force Policy. He also alleges that the personnel who evaluate the exercises are not adequately trained or qualified as evaluators and do not have a comprehensive understanding of the Deadly Force Policy. He further states that, at times, administrative staff had conducted the evaluations of the exercises. According to the informant, these factors diminish the value of the evaluations.

Response 4: 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. This is not true. Since some exercises have specific functions, the cost to gather all of the information is not justified. Many exercises are run to understand or develop protection strategy. 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. Of course, all exercises offer an opportunity to learn. When errors by security force personnel are noted, they are typically corrected by the appropriate security supervisory personnel on the spot.

While security personnel are always involved in the running of a MILES exercise, the number of exercises and the different purposes means that different personnel are used to assist in the process. There will be situations where all parts of the security staff, to include administrative personnel, are involved in exercises and in the evaluation. The use of a wide variety of personnel does not diminish the value of the evaluations; rather it helps improve it since there are different viewpoints brought to the event.

Since the beginning of the use of MILES equipment, safety has been a major emphasis. There is a formal process that is focused on ensuring all force-on-force exercises are run in a safe manner. The DOE employs formal processes for handling both weapons and ammunition. Safety monitors, as well as performance monitors, ensure that the process is conducted in a safe manner. DOE guidance for planning and conducting MILES-enhanced Force-on-Force exercises requires that all Controllers/Evaluators receive formal training in their various responsibilities. For reasons of safety and control, some large-scale exercises require large numbers of Controllers, sometimes necessitating the use of "non-tactical" personnel – such as administrative or logistics- for some positions. However, tactically qualified personnel (including protective force members and supervisors) are typically assigned to Controller positions requiring tactical knowledge (including knowledge of deadly force policy) and to Evaluators positions. Some organizations, to include the Office of Secure Transportation, commonly use outside tactical experts (e.g. military) to assist in evaluating performance during exercises.

Allegation 5: *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.*

DELETED

The tests also fail to compensate for the lack of surprise. The claimant states that the protective forces who serve as the "adversaries" lack the training necessary to simulate terrorist's capabilities in these exercises.

Response 5: The informant's information is incorrect. The DOE has, and continues to, run exercises that would address the most severe of the 'real' adversary situations.

DELETED

DOE does limit the adversary equipment to that which is available in the world market. The decision on what equipment is available is defined by the intelligence community.

The claimant is correct in stating that certain situations (including speed, surprise, and violence of action) cannot be tested through force-on-force testing due to safety concerns and practicality. High-speed vehicles and actual use of certain gases and explosives must be simulated. The elements of surprise and violence of action, while clearly anticipated in an actual event, are difficult, if not impossible, to simulate during scheduled training exercises. The DOE is aware that this places limitations on the exercise. However, in order to have a safe facility, certain limitations are placed on exercises. The exercise is only part of the whole protection strategy and, as such, these limitations are acceptable.

The claimant raised a question on the adversaries that are used for the exercises. The DOE works with the Department of Defense (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.

When the Office of Independent Oversight and Performance Assurance conducts force-on-force performance tests, it uses a Composite Adversary Team composed of highly skilled Security Police Officers from various DOE/NNSA sites who undergo additional advanced training in the planning and conduct of offensive operations, including the use of rapid hard-hitting shock tactics, force multipliers, and specialized weapons and explosive devices.

The new vulnerability tool (Iterative Site Analysis) being used in the NNSA uses personnel who have the knowledge referred to by the informant. The adversaries selected for these tabletop exercises bring with them experience that is as close as possible to the potential adversaries that might attack a DOE facility. The ISA process requires them to identify not only what they would do at a site, it requires identification of how they would plan for the attack and how they would obtain and stage the materials. There are no limitations placed on the adversaries other than use of materials that are currently available in the world to potential adversaries. This process helps the DOE validate that the overall security posture is adequate to address the current threat.

Additionally, the Department of Energy has one of the most extensive set of force-on-force programs within the government.

Allegation 6: The claimant also alleges that no adjustment is made to the result of the performance test when the exercise is compromised or cheating is discovered, nor does DOE investigate instances of cheating. As an example, he cites an incident involving a performance test for the Office of Transportation Safeguards conducted in 1999 at Ft Hood, Texas. In that case, he alleges, the protective force was discovered cheating, yet no investigation into the security breach was conducted, nor was the cheating factored into the results of the exercise. Instead, he states, DOE recorded the exercise as a "win" for the protective force. The claimant alleges that the failure to account for these variables in the results of the performance tests produces unreliable and artificially inflated test results.

Response 6: This allegation is based on an event that has been reviewed in the past by the DOE. The allegation deals with a Joint Training Exercise with the State of Texas law enforcement and emergency management, Fort Hood military and other organizations in 1999 conducted at Fort Hood. During the exercise, the Transportation Safeguards Division (TSD) forces were successful in repelling an attack from the U.S. Army Special Forces mock "terrorists." An allegation was made by one of the Special Forces members who reportedly had discovered that the TSD forces had acquired a paper copy of the mock "terrorist" plan for the exercise, and had used it to cheat.

On the two occasions when the DOD Special Forces member made this statement to Office of Transportation Safeguards (OTS) management, he would not provide any specific details. The Exercise Director asked the Special Forces member specifically who was cheating and the Special Forces member refused to provide the requested information. The Exercise Director advised the Special Forces member it would be difficult to follow through without identifying the individual accused of cheating. The Exercise Director held a meeting with all exercise controllers, including the Opposition Force Lead Controller, and conducted an informal inquiry. None of the controllers, including the Opposition Force Lead Controller had observed, nor was aware of, any individual having used a paper copy of the mock "terrorist" attack to cheat during the exercise.

Without additional information, the inquiry was closed. The purpose of this exercise was to develop a better working relationship with state law enforcement and emergency management. This was not a 'rated' exercise that is part of the formal validation process for TSD. While the allegation was taken seriously and cheating is not tolerated, no additional action could be taken since there was no additional information provided by the DoD Special Forces member.

Allegation 7: The claimant alleges that the DOE does not routinely use computer modeling of protective force tactics as a means of evaluating protective force engagements. He notes that computer modeling is an effective means of simulating protective forces response to worst case scenarios. He states that when DOE does conduct computer modeling it uses an older system known as the Joint Tactical Simulation (JTS) system. According to the informant, DOE has identified significant errors in the database for the JTS combat simulation which make JTS an inadequate tool

for computer modeling.

DELETED

Response 7: The DOE not only uses computer evaluations, but also is working on the next generation of computer modeling to support evaluations of its sites. The claimant is correct in noting that JTS was one of the first evaluation tools. It is a very basic computer simulation. The errors in the database dealt with the computer calculation of probability of firing certain weapons and hitting a target. These errors have been corrected.

DELETED

It should be noted that computer simulation is only one of the tools used to help define the protection strategy for a site. It can be a cost-effective tool in developing and evaluating a variety of potential protection strategies. DOE is working on developing the next generation of computer simulation software that will use the type of computer engines that are being used in commercial computer gaming software. Since the DOE deals with classified information, the transition from the commercial world to the classified world will take some effort.

***Allegation 8:** 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 the basis for its annual report to the President and Congress on the state of DOE's ability to protect its facilities.*

Response 8: The previous discussion notes that the informant's information is dated and does not reflect current efforts. While there is no perfect security system, the DOE has taken all of the steps necessary to ensure that the protection strategies and the actual protection in place would provide the high level of assurance needed for the materials in the custody of the DOE. It is through the use of all of the tools in the security arena that allows the DOE to support its annual report to the President. 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.

Alleged Deficiencies In DOE Safeguards And Security

Allegation 9: 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.

Under the Safeguards and Security Program, the contractors at the local facilities conduct self-assessments which cover the following areas: 1) program management 2) protection program operations, 3) information security, 4) nuclear material control and accountability, and 5) personnel security. The contractor uses the self-assessment in the management of the facility and as the basis for corrective actions or changes in the facilities operations.

The local DOE officials, under the auspices of the DOE's Safeguards and Security Program, inspect and evaluate a facility's operation in the same subject areas reviewed by the contractor. They use the contractor's self-assessment to perform their annual Safeguards and Security Survey. After the local DOE officials review the facility they assign it a composite security rating.

To support his allegations that the reliance on contractor self-assessments and local review is inadequate to ensure the security of the facility, the claimant cites his own experience. He states that between 1995 and 2000, under the former Quality Assurance program managed by DOE headquarters, he consistently noted facility vulnerabilities that should have been identified in the safeguards and security surveys, that had not been. Some of the vulnerabilities he noted in his reports included situations where protective force responders did not know where to go when there was an emergency, did not know when to use deadly force, and did not know where the Special Nuclear Material was kept at the facility. Despite these deficiencies, these facilities reported successful performance tests in the safeguards and security surveys.

In addition, during the same time period, the claimant personally reported, in classified documents, numerous high-risk conditions and vulnerabilities to senior DOE safeguards and security managers. These classified reports involved several facilities but primarily focused on the Office of Transportation Safeguards, the Rocky Flats Environmental Technology Site and the Los Alamos National Laboratory. The claimant states that, to date, he is not aware of any actions taken by DOE to resolve those high-risk conditions. A list of classified reports was provided along with a document confirming their delivery to a senior official in DOE's security office

The claimant alleges that, as the pace of oversight inspection has decreased, so has the rate of findings and deficiencies reported by the safeguards and security surveys. Thus,

from 1986-1991 when independent oversight inspections by DOE Headquarters were frequent and comprehensive, approximately 1000 findings and deficiencies were noted annually by the oversight inspectors. During the same timeframe, the DOE Safeguards and Security surveys identified approximately 4000 findings and deficiencies annually. He points out that since 1991, the number and scope of oversight inspection has steadily decreased. As a result, the findings and deficiencies identified by the oversight inspections have dropped to approximately 250 annually. Significantly, according to the informant, the deficiencies identified by the DOE's Safeguards and Security surveys have also dropped to approximately 1000 annually. According to the informant, the sudden decrease in the number of findings and deficiencies in the surveys shows that without regular oversight inspections, DOE's Safeguards and Security program process is even less reliable.

The claimant states that the inspectors recommend the composite security rating for the facilities, but the local DOE managers may assign another rating if they choose to. He alleges that this highlights the need for independent oversight of this process that could establish one final, official security rating that would be based on one set of standards.

Response 9: The claimant identifies a number of allegations dealing with oversight of safeguards and security. 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. DOE has two separate organizations that provide these centralized inspections. The first is the Inspector General (IG). This DOE organization is consistent with its government-wide mandate and it looks at a wide variety of security areas. During 2001 & 2002, the IG conducted seventeen reviews/inspections that addressed security issues.

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 and security. This office conducts inspections of those facilities with Category I quantities of Special Nuclear Material on a regular basis. The frequency is dependent on the level of performance at the last formal review. The minimum frequency is bi-annual. If there is a specific concern or a defined weakness, assessments will be more frequent.

In addition to the headquarters oversight, the DOE relies on a graded level of oversight. The first level of oversight is the DOE contractor. DOE contractors are required to conduct self-assessments of their safeguards and security protection. The contractor is the entity that actually implements security and, as such, it is appropriate to have an internal assessment capability. This also provides the contractor an opportunity to question the requirements.

The DOE has federal personnel who are assigned the on-site responsibility for security. The manager of the federal site office is required to conduct an annual assessment of the

contractor. The claimant alleges that the DOE only uses the contractor's self-assessment. In fact, the federal official conducts an independent review of the site. In the past, this was a two-week effort. Over the past two years, a few of the federal site offices have been transitioning to a continuous review process throughout the year. The results of either a focused two-week or continuous review are summarized at one time for the contractor. The contractor's self-assessment is reviewed against the results of the federal oversight inspection. This data is used as input to the performance appraisal of the contractors.

The National Nuclear Security Administration is in the process of completing its re-organization. The oversight and assessment policy that is being established places more responsibility on the field. Thus, the contractor's self-assessment and the annual federal inspection meet this policy objective. Headquarters NNSA personnel are responsible to ensure that the federal field office is performing its function. As noted above, there are two other headquarters organizations that perform inspection of the contractor's activities. The NNSA headquarters organization uses these reviews as part of its oversight of the federal and contractor efforts.

The allegations about previously reported security conditions and vulnerabilities are based on dated information that has been superseded by more recent evaluations and protection strategies. When security vulnerabilities were identified they were corrected in a timely manner. The incumbent would not have been provided the results of many of the fixes due to his loss of security clearance and lack of need-to-know. The Office of Transportation Safeguards has had numerous reviews and upgrades since the information referenced by the informant. Additional details on Los Alamos National Laboratory are provided in the response to separate questions.

The claimant alleges that a decrease in the number of findings from 1986 indicates a problem. He fails to note that there has been a significant reduction in the number of facilities and areas within the remaining facilities that handle sensitive information. DOE has shut down a number of sites (Mound, Pinellas). Other sites are in the process of shutting down (Rocky Flats, Richland). The Nevada Test site is no longer testing nuclear weapons. Other sites have had the number of locations on-site, with sensitive information or materials, reduced (Los Alamos National Laboratory, Sandia National Laboratories, Idaho National Engineering and Environmental Laboratory). It should be expected that with fewer sites there would be a significant reduction in both the number of inspections as well as in the number of findings.

The claimant also questions the ratings provided by the field offices. The claimant is apparently referring to a specific event. The DOE IG reviewed this allegation and issued a report (Report IG-0471, Inspection Report on "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", dated May 2000). The IG report noted that while there were reasons for the changes in ratings, the field office had not documented those reasons very well. There were no violations of law or regulations in that event.

A fundamental change made within the Safeguards and Security program in the Department of Energy was to ensure that authority and responsibility were consistently implemented. The Department of Energy approach is to place the inspection process into two organizations. While anyone can provide information to these organizations, these organizations are responsible for evaluations. The change in the informant's responsibilities appears to be due to changes in the organization's roles. The informant's opinion on what is high risk may not necessarily match the criteria used by those who have the authority and responsibility for this area.

Allegation 10: *Another concern the claimant raises about the effectiveness of the inspection process is that the facility vulnerability assessments that contractors prepare are not shared with the inspectors conducting the annual safeguards and security surveys. The vulnerability assessments contain the key assumptions about a facility's weaknesses which are used to build a protective strategy. These assumptions concern issues such as the probability of detecting weapons, and the time necessary for an adversary to gain entry to a vault, acquire the nuclear material and escape. The assumptions also concern the amount of time necessary to create an improvised nuclear device or sabotage the facility.*

It is the informant's contention that not informing the DOE inspectors of the assumptions in the vulnerability assessment seriously hampers the process because it results in the inspectors conducting the survey with incomplete data. He emphasizes that the survey program is the key to the assessments and security analyses. Because the inspectors are working with incomplete information, he alleges, they are not able to properly evaluate the facility's readiness to withstand an attack, and may assign a composite security rating that does not accurately reflect the state of the facility.

The claimant also states that DOE headquarters no longer conducts independent review 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.

Response 10: The claimant is relying on dated information. The DOE inspectors (federal field office personnel, the Inspector General or the Office of Independent Oversight and Performance Assurance) have access to Vulnerability Assessment (VA) information. In addition, the federal site personnel are involved in the development of the VA and in the approval of the SSSP that relies on the Vulnerability Assessment. The Office of Independent Oversight is invited to, and has participated in, the new Iterative Site Analysis process that will become one of the main analytical tools of the Vulnerability Assessment. This allows the inspectors to have access to the Vulnerability Assessment. There have been no issues raised by any inspectors in the last two years over access to Vulnerability Assessments.

Allegation 11: *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. In other words, the inspection duty is an "other duty as assigned." In addition, some of the survey team members lack the technical background and expertise for testing the effectiveness of DOE's complex alarm systems and methods to circumvent them. As a result, DOE inspectors do not always have the appropriate expertise and training to properly evaluate the facilities.*

DOE Order 470.1 specifies that survey team personnel shall, among other things, have sufficient training to perform effective and thorough surveys. It also states that new inspectors must attend basic survey training. According to the informant, as of August 2000, less than 50% of the inspectors had received the training for this duty offered by DOE. Moreover, the claimant notes that because the inspection duties are considered merely ancillary responsibilities, the inspectors themselves are not eligible for the training. As a result, the lack of training is a continuing problem.

Response 11: In fiscal years (FY) 2001 and 2002 and FY 2003 to date: 164 DOE personnel have taken the basic survey training course and 295 have taken the introduction to the survey procedure course. In addition, 69 personnel have taken the advanced courses (Protective force (20), survey of systems (31), and survey team leader (18)). There may be some individuals who are put on the team as part of on-the-job training or to provide a better understanding of the security issues; however, these are limited in numbers and additional experienced and qualified personnel are on the team to ensure all areas are adequately addressed. Also, additional resources are available to augment the team when necessary. Headquarters, other site offices and contractor resources can and have been used to provide the required expertise.

The claimant appears to be relying on a specific issue that was raised over the reviews conducted by one DOE office in 1999. This issue was addressed in a DOE Inspector General Report (DOE/IG-0471) titled "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" dated May 2000. That issue has been specifically addressed and the site requires training for all inspectors prior to participating on the review teams.

Allegation 12: *The claimant states that DOE does not conduct unannounced inspections as a component of its safeguards and security program. According to the informant, certain activities such as protective force operations, including whether patrols are being conducted as required, and response to alarms should be reviewed and evaluated on an unannounced basis. The claimant alleges that the failure to conduct unannounced inspections results in inadequate evaluations of facility defense operations and artificially high estimates of defense preparedness.*

Response 12: The DOE does not require, nor routinely conduct, unannounced force-on-force inspections due to the difficulty in conducting these exercises and the concern over

safety. The force-on-force exercises must be announced in order to ensure personnel are available to provide security during the exercise, as well as to ensure the exercise is run safely. Other testing of the protective forces has similar limitations.

The continuing survey program, that a number of DOE Federal site offices are moving toward, is the equivalent of unannounced inspections. The Federal personnel request the site to test its personnel on selected security force responsibilities on a random basis. This random testing is conducted on selected areas at selected DOE sites. Not all performance tests can be conducted in this manner.

This overall allegation is fundamentally incorrect in that it implies that the security force will not follow the rules unless there is someone continually watching over them. The DOE security force is a highly trained and motivated security organization. The implications of this allegation are not representative of the high level of professionalism that exists in the DOE security protective forces.

The Department of Energy's actions on unannounced inspections are consistent with the approach used by most government agencies. It is noted that DOE runs more exercises than other government agencies that protect equivalent materials and information.

***Allegation 13:** The claimant also alleges that DOE headquarters personnel assigned security management responsibilities for major nuclear facilities often lack the necessary qualifications and training for security matters. He notes that in one particular case, a physical scientist was assigned the safeguards and security responsibility for two nuclear facilities.*

Response 13: The decision on assigning personnel security management responsibility in the DOE follows the requirements to select the most qualified personnel for the identified position. The DOE follows the formal selection procedures and requirements for federal employees as set forth by the Office of Personnel Management. The claimant appears to be concerned about the qualifications of two individuals. Generally, it is noted that the current personnel in safeguards and security have a wide variety of backgrounds. They include personnel who are engineers, lawyers, statisticians and former police officers. Some job descriptions for security personnel include requirements for physical scientists in order to obtain the necessary interface with the actual operation of a site. Another example is the use of statisticians for Material Control and Accountability. Management of security is not limited to any one background. Personnel from operations are encouraged to work in security, if only for a short time, in order to understand better the issues that must be dealt with in security.

An issue that the claimant may be alluding to is the level of training of the individual who had a specific position. While many individuals in security have learned their jobs through on-the-job training, the DOE does have its own security training academy (Non-Proliferation and National Security Institute). This academy provides training on all

aspects of security to support both the DOE and other agencies. Thus, an individual can be selected for a position based on being the best choice and then additional training can be made available within the DOE.

Thus, the specific concern that an individual who was a physical scientist was assigned responsibility for management of security is misplaced. The DOE will continue to follow the requirements for selection as defined by OPM and will provide specific training to ensure that the DOE employees have the knowledge needed to carry out their specific responsibilities.

Under separate correspondence, the claimant provided the names and positions of the two individuals alluded to in the original report as "lacking the necessary qualifications" and being "assigned the safeguards and security management responsibility for two nuclear facilities." It should be noted that these individuals worked in an organization within the Department of Energy that did not have direct programmatic authority or responsibility for the implementation of safeguards and security.

Allegation 14: *The claimant observes that responsible officials frequently fail to make necessary entries into the DOE's Safeguards and Security Information Management Systems (SSIMS). SSIMS is the tracking system for findings and deficiencies and corrective actions needed at DOE facilities*

The claimant alleges that SSIMS is not used and updated in accordance with DOE Order 4701. The Order requires that SSIMS reflect facility information, activity information and survey information. It also requires that SSIMS entries be made as conditions at the facilities change and corrective actions are taken. The claimant alleges that the responsible officials frequently fail to enter findings in SSIMS and fail to devise and implement corrective actions as needed. The failure to develop and implement corrective actions for noted deficiencies, he alleges, unnecessarily degrades national security. Examples of unclassified SSIMS entries the claimant identified as matters of concern were provided as an exhibit.

Response 14: The SSIMS is an administrative reporting tool that assists management at Headquarters in tracking findings developed in the field and Headquarters facilities. While there may have been some delays in updating the SSIMS records, it is misleading to assume the lack of documentation in SSIMS is indicative of poor security at the sites. As discussed earlier, federal field personnel are responsible for monitoring the contractor's performance and monitoring corrective actions. The fact that there are outstanding issues in SSIMS is not, in and of itself, an indicator of an unhealthy safeguards and security program. Closing out the reporting system is important to ensure all appropriate personnel are aware of the solutions; however, the SSIMS system does not, by itself, fix anything.

A review of the incidents provided by the claimant does not identify any that currently question the level of protection of the DOE complex. In addition, the tracking process is working, since the majority of these items have been closed out. The Department of

Energy has undertaken efforts to computerize the incident response data in a manner that will allow both the field and headquarters to use the data better. This has resulted in a better understanding of issues that have been completed, but the system has not kept up with the changes. DOE is expending effort to ensure that the new computerized system is current and useful to managers in order to track incident reports. This is an evolving effort, but is an indication that the DOE takes the tracking of incidents seriously.

Allegation 15: *The claimant alleges that serious deficiencies in DOE's assessment and management of security risks identified by the Office of Inspector General in a report dated September 2000 have not been resolved. Specifically, the informant alleges that DOE has not 1) implemented the new safeguards and security process noted in the report as the solution to problems identified, 2) established a policy on what actions are required when moderate and unacceptable or high risk conditions have been identified; 3) developed a dispute resolution process to resolve technical difficulties regarding risk determinations; and 4) resolved the unacceptable or high risk conditions in the allegations made to the OIG.*

Response 15: The claimant appears to be referring to the Inspector General report DOE/IG-0482 of September 2000 entitled "Summary Report on Allegations Concerning the Department of Energy's Site Safeguards and Security Planning Process." This report states:

"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 SSSP's. 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."

The restructuring of the SSSP process has been completed with the publication of the "Format and Content Guide for Site Safeguards and Security Plans". The draft was issued in March 2000 and was finalized in March 2001. The events of September 11, 2001, and the introduction of potential changes in the threat, delayed the publication of a revised process. It is noted that the establishment of the National Nuclear Security Administration (NNSA) through Public Law 106-65, clarified some of the organizational relationships that led to the original issues. The law clarifies that the Safeguards and Security policy is developed by the Office of Security (SO) who is a direct report to the Secretary. The implementation of the policy for the nuclear weapons complex is accomplished by the NNSA. Thus, the acceptance of risk and the risk determinations are now clearly decisions within the purview of the NNSA. Since the process requires those federal individuals responsible for risk acceptance to sign the SSSP, the basic issue of resolving disagreements has been resolved.

The Alleged Security Risks At The Los Alamos National Laboratory

Allegation 16: *The claimant alleges that there are serious problems at the Los Alamos National Laboratory (Los Alamos).*

Los Alamos is located approximately 93 miles north of Albuquerque and has multiple, distinct security areas connected by public roads. Each area is a stand-alone facility for the purposes of security and protection. Each area is also staffed by its own guards who provide security at the points of entry. The claimant notes that the Special Nuclear Material is distributed among several areas. Most of the storage facilities for the Special Nuclear Material are not hardened, nor are many of the vehicles used by the protective personnel who patrol Los Alamos.

The claimant observes that because there are public roads and mountainous terrain included in its physical layout, Los Alamos is a more vulnerable facility than one which is contained in a single area. He states that there are only minimal delay mechanisms built into the facilities to stop or stall intruders from entering the distinct, secure areas. He also states that Los Alamos has only one protective response team. This team is tasked with protecting and defending the facility in the event of an attack.

Pursuant to DOE Order 470.1, a facilities protective force must be able to respond to the area under attack before the adversary gains entry to the targeted building. Based on the information provided by the informant, it is alleged that the protective force at Los Alamos frequently loses the force-on-force exercises, thereby failing to defend the facility.

Moreover, according to the informant, the remote location of some of the technical areas and their position in a canyon are additional hurdles to the defense of Los Alamos. The claimant states that these factors complicate the job of the protective response team because if they are drawn to the site of a disturbance that turns out to be merely a diversion, they may be trapped and unable to respond to a real attack in a different secure area. Given these factors and the size of the Los Alamos facility and its response team, the claimant alleges that the security is inadequate to protect and defend the facility and its nuclear assets. As a result, he alleges that the protective response team cannot respond in a manner that complies with the Order.

Response 16: The claimant has correctly identified the Los Alamos National Laboratory facilities as difficult to protect. The claimant is not aware that the number of locations of concern has been reduced over the last two years. The claimant is also not aware of the current protection strategy that allows the site to provide the level of protection needed to address the Design Basis Threat.

The claimant no longer has a security clearance or a need-to-know for current information on the status of the security for this or any other DOE site. Thus, the claimant is not aware of the significant improvements that have been made in the security posture of these facilities that are potential targets or the details of how the security force deploys and responds to events. He has made statements that are not correct today. Over the last two years, significant changes have been made that have improved the protection

of the facilities that are considered targets. These changes have addressed all of the concerns identified by the informant. These changes include classified details on protection strategies for which the claimant would not have a need-to-know. Recent inspections by DOE have revalidated that the level of protection currently being provided meets the DOE requirements. The allegation that the security is inadequate is incorrect.

While the protection is adequate, there are other actions ongoing at LANL that will impact the security of the facility. A study was conducted to identify the best option on the future location for a number of experimental facilities that are currently located at LANL. The business-case analysis determined that it is appropriate to move a number of experimental facilities to the Nevada Test Site. While security was part of the analysis, the major deciding factor had to do with the future best business case analysis of how work will be done in the future in the nuclear weapons complex. Moving the experimental facilities and their associated nuclear materials will reduce the number of facilities that require a high level of security needed for special nuclear material at LANL. This effort to move the experiments will take significant time due to the need for a construction project. The future security of these experiments is expected to be easier to maintain since the new facilities were designed with the intent of providing a high level of security.

Alleged deficiencies and security risks by the Office of Secure Transportation.

Alleged deficiencies and security risks by the Office of Secure Transportation were provided by the claimant under separate correspondence. It is noted that the Office of Special Counsel had previously requested a response to some of these concerns in an earlier request from National Security Advisor Condoleeza Rice to Department of Energy Secretary Spencer Abraham citing an identical OSC file number reference. The response to these issues is classified and will be provided under separate cover.

ATTACHMENT I

SITE SAFEGUARDS AND SECURITY REQUIREMENTS

DOE Order 470.1 requires a Site Safeguards and Security Plan (SSSP). This plan is the master planning document that is prepared for the following sites:

1. Those sites with facilities that possess a Category I quantity of special nuclear material, or those that have Category II quantities within the same Protected Areas that roll up to a Category I quantity.
2. Those sites 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.
3. Those sites that have an industrial sabotage threat that would cause an unacceptable impact to those DOE programs supporting national defense and security.
4. Other facilities/sites that Heads of DOE Elements deem appropriate.

The SSSP shall contain information that describes:

1. Protection strategies.
2. Site 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 risk.
 - 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.

Office of Secure Transportation
Response to OSC File No. DI-02-0572 (U)
Revision 1
March 24, 2003

(U) The following is a response on the behalf of the NNSA Office of Secure Transportation (OST) to allegations made on January 15, 2002, as part of the OSC File No. DI-02-0572. Only those allegations that are specifically related to the OST mission are addressed.

(U) The response corresponds to the sections of the original report.

Introduction: (U) There are no OST specific matters in this section.

Section 1: (U) The informant stated that DOE's class "A" nuclear research facilities and laboratories are required by DOE Order 470.1 to use explosive detection equipment at certain points of entry.

- ~~(S)~~ OST is not a class A facility.

DELETED

OST continues to monitor and encourage development of HE detection equipment with sufficient fidelity to meaningfully support the mission.

DELETED

DELETED VERSION

U.S. Department of Energy Declassification Review	
1 st Review Date: 02/08/2005	Determination (Circle Number (s))
Authority: <input type="checkbox"/> AOC <input type="checkbox"/> DC <input checked="" type="checkbox"/> ADD	1. Classification retained.
Name: Michael L. Gates	2. Classification change to: _____
	3. Contains No DOE Classified Info.
2 nd Review Date: 02/09/2005	4. Coordinate with: _____
Authority: ADD	5. Classification cancelled.
Name: Charles L. Trujillo	6. Classified Info. Bracketed
	7. Other (Specify): _____

Classified by: J.P. Ch. Avang Director, LSAD, 012403
Declassify on: OADR, December 2008
Declassify on: N/A

~~SECRET~~

DELETED

- ~~(S)~~ adversary and protective force personnel agree on simulated weapon capabilities Both prior to exercises.

DELETED

- ~~(S)~~ OST security evaluation scenarios are based on extensive analysis and testing of the entire transportation mission.

DELETED

~~SECRET~~

~~SECRET~~

DELETED

~~SECRET~~

~~SECRET~~

DELETED

- (U) Data collectors' brief information acquired during the scenario based on the prescribed data collection forms. Additional insights on tactical behavior and key events are also captured on videotape for later analysis. The synthesis of all such data is reported and evaluated for every exercise. If inappropriate controller calls or player (adversary or protective force) behavior may have had a significant enough effect to influence the outcome of an exercise, then the exercise is void and no credit, positive or negative, is taken in evaluating security effectiveness for that exercise. Exercises have been declared void for these reasons in recent FoFs in order to ensure the integrity of the OST risk evaluation process and results.

DELETED

- ~~(S)~~ The alleged "performance test compromise" in Ft. Hood in 1999 has been addressed in many previous responses of this nature. Because there ~~are~~ ^{is} no formal allegations made that indicated specific personnel ~~that~~ may have been involved, it was not possible to take specific action in that particular matter.

Jan
77

DELETED

- ~~(S)~~ It is true that it is extremely difficult to replicate the element of surprise that the protective force might experience in the event of an actual terrorist attack. This situation is partially addressed by firm ROEs requiring that protective force personnel not "lean forward" inappropriately prior to start of an exercise.

DELETED

- ~~(S)~~ Further compensation for the lack of surprise is provided by the adversary's precise knowledge of convoy arrival time at a particular location, which again, because of the random nature of the flow of events of convoy operations, would be extremely difficult to accurately predict.
- ~~(S)~~ In addition, no credit for preemptive detection prior to attack is taken when evaluating OST security effectiveness. Such detection could occur by either the protective force or by civilians. In reality civilian detection would be a

~~SECRET~~

~~SECRET~~

significant impediment to adversary site preparations and movements prior to attack onset -- again, no credit is taken other than trying to ensure that attacks are planned with minimal probability of detection.

- ~~(S)~~ Matricide is a very serious concern for any operation and OST is certainly no exception.

DELETED

- ~~(S)~~ OST continues to consider and evaluate new and emerging potential threats against their convoy operations.

DELETED

- ~~(S)~~ OST routes are selected to minimize vulnerabilities to their operation and our citizens.

DELETED

~~SECRET~~

~~SECRET~~

DELETED

~~(S)~~ The following is a one-to-one response to each of the items in the clarification section related to Section 2 titled "OTS Concerns".

DELETED

Response: It is true that there is some predictability to OST routes and sub stops, since OST operates on public highways and there are only so many reasonable routes between any two locations.

See
M.

DELETED

~~SECRET~~

~~SECRET~~

DELETED

7) *Issue: GTS SA's do not wear uniforms.*

DELETED

Response: It is true that OST federal agents do not wear uniforms.

DELETED

~~SECRET~~

~~SECRET~~

DELETED

Response: OST federal agents routinely practice link-up with LLEA in FoF exercises and provide compatible communication systems and techniques. OST has a strong liaison program that educates state and local law enforcement along primary shipment corridors including the maintenance of State-level Law Enforcement and/or Emergency Management Center points-of-contacts.

DELETED

12) Issue: MILES rules of engagement are unrealistic.

DELETED

Agreement
between both sides is obtained prior to exercises. This is true for all activities, sensitivity analysis, or system validation.

DELETED

~~SECRET~~

~~SECRET~~

DELETED

~~SECRET~~

DELETED

Section 4: ~~(S)~~ The informant alleges that DOE does not keep accurate records of protective force performance in these force-on-force exercises. For example, DOE does not keep records of losses sustained by the protective force, errors made by the protective force, fratricide by members of the protective force, or other violations of DOE's Deadly Force Policy. He also alleges that the personnel who evaluate the exercises are not adequately trained or qualified as evaluators and do not have a comprehensive understanding of the Deadly Force Policy. He further states that, at times, administrative staff had conducted the evaluations of exercises. According to the informant, these factors diminish the value of the evaluations.

• ~~(S)~~

DELETED

All controllers and evaluators are trained in the exercise ROEs and in the data collection process.

Section 5: ~~(S)~~ Additional issues of concern raised by the informant involve the structure of performance tests. He notes that the exercises do not replicate real adversary situations.

DELETED

Section 6: ~~(S)~~ The informant alleges that no adjustment is made to the result of performance test when the exercise is compromised or cheating is discovered, nor does DOE investigate instances of cheating.

• (U)

DELETED

Instances when inappropriate controller calls or player behavior (adversary or protective force) could have made a significant difference in the scenario outcome are noted and the exercise results are voided—no credit, positive or negative, is taken for such exercises.

Section 7: ~~(S)~~ The informant alleges that the DOE does not routinely use computer modeling of protective force tactics as a means of evaluating protective force engagements.

~~SECRET~~

DELETED

Section 8: ~~(S)~~ *The cumulative effect of these deficiencies, according to the source, degrade the value of performance tests.*

DELETED

OST has a proactive track record of anticipating threat conditions before they become requirements and voluntarily assessing themselves against higher than mandated threat conditions.

Section 9: ~~(S)~~ *The informant 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.*

- DOE Office of Independent Oversight and Performance Assessment (OA) regularly observe OST exercises and security evaluation planning and processes. Additionally, there is an identified trusted agent from OA on the OST SSSP Working Group.

Section 10: ~~(S)~~ *Another concern the informant raises about the effectiveness of the inspection process is that the facility vulnerability assessments that the contractors prepare are not shared with the inspectors conducting the annual safeguards and security surveys.*

- As appropriate, OST shares VA results with safeguard and security survey personnel. The OST SSSP Working Group has such external membership identified as trusted agents.

Section 11: ~~(S)~~ *The informant 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.*

- (U) This is a DOE HQ topic and not applicable to OST.

Section 12: ~~(S)~~ *The informant states that DOE does not conduct unannounced inspections as a component of its safeguards and security program.*

DELETED

~~SECRET~~

~~SECRET~~

DELETED

Section 13 ~~(S)~~ The informant also alleges that DOE headquarters personnel assigned security management responsibility for major nuclear facilities often lack the necessary qualifications and training for security matters. He notes that in one particular case, a physical scientist was assigned the safeguards and security responsibility for two nuclear facilities.

- (U) This is a DOE-HQ topic and not applicable to OST.

Section 14 ~~(S)~~ The informant observes that responsible officials frequently fail to make necessary entries into DOE's Safeguards and Security Information Management Systems (SSIMS).

- Prior to the NNSA Reorganization, OST provided the required input to the local Albuquerque Office for input. Subsequent to the reorganization, OST now maintains this responsibility.

DELETED

~~SECRET~~



~~SECRET/NOFORN~~
Department of Energy
National Nuclear Security Administration
Washington, DC 20585
SEP 27 2002

OFFICE OF THE ADMINISTRATOR

The Honorable Condoleezza Rice
National Security Advisor
The White House
Washington, D.C. 20500

Re: OSC File No. DI-02-0572

Dear Dr. Rice:

In response to your request to the Secretary of Energy of August 9, 2002, the Department of Energy/National Nuclear Security Administration (NNSA) has reviewed the concerns and allegations presented to the U.S. Office of Special Counsel, File No. DI-02-0572. The allegations have been carefully reviewed and are based on information that is at least five years old and is now no longer accurate. The National Nuclear Security Administration's Office of Transportation Safeguards' highest priority is to ensure the safe and secure transportation of nuclear material, nuclear weapons components, and nuclear weapons. The Office of Transportation Safeguards, through self assessments and inspections from independent teams, is continuously evaluating and, when necessary, upgrading the physical security afforded to shipments of special nuclear materials, nuclear weapons components, and complete nuclear weapons in transit between Department of Energy sites and to/from Department of Defense installations.

The issuance of Presidential Decision Directive-39, "U.S. Policy on Counter-Terrorism," directed enhanced capabilities for the Office of Transportation Safeguards. To meet this requirement the Office of Transportation Safeguards designed, tested, and deployed a Special Response Force. The Special Response Force greatly enhances the security posture through the use of: (1) additional agents, (2) specially modified support vehicles, (3) enhanced offensive capabilities, and (4) enhanced tactical training and tactics. Further enhancements have been implemented as a result of the September 11 attacks so that the Office of Transportation Safeguards security profile is the strongest it has ever been.

Based on a detailed review, I can assure you that the all the allegations expressed are unfounded, given the strong position of today's Office of Transportation Safeguards. The Department of Energy/National Nuclear Security Administration is confident that the Office of Transportation Safeguards is well equipped, trained, and prepared to protect its cargoes in the interest of national security. Enclosed is the Department of

~~SECRET/NOFORN~~

~~Document(s) Transmitted herewith contain(s)
NATIONAL DEFENSE INFORMATION~~

This page unclassified when separated from the attachment

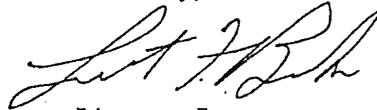
~~SECRET/NSI~~

Energy/National Nuclear Security Administration's paragraph-by-paragraph response to the concerns presented in the U.S. Office of Special Counsel, File No. DI-02-0572.

The Department of Energy's Office of Independent Oversight and Performance Assessments conducts routine independent assessments of the Office of Transportation Safeguards and has verified the effectiveness of the Transportation Safeguards System, including the Special Response Force. The Office of Independent Oversight and Performance Assessments reports directly to the Secretary and is completely independent of the National Nuclear Security Administration. Its most recent assessment was conducted from August 25 to September 20, 2002. To ensure an independent evaluation of the allegations presented to the Office of Special Counsel, I requested the Office of Independent Oversight and Performance Assessments to explicitly examine those allegations during its assessment. Their conclusion was that "while some of the allegations may provide broadly accurate representations of past issues, these issues were addressed some time ago." Their specific findings are consistent with those in the enclosed paragraph-by-paragraph response.

In the event you require any additional information or desire a briefing on the Office of Transportation Safeguards operations, please do not hesitate to have your staff contact me at (202) 586-5555.

Sincerely,



Linton F. Brooks
Acting Administrator

Enclosure

~~SECRET/NSI~~

~~Document(s) Transmitted herewith contain(s)~~

~~NATIONAL SECURITY INFORMATION~~

This page unclassified when separated from the attachment

DOE RESPONSE TO
CLASSIFIED MEMORANDUM
FROM
U.S. OFFICE OF SPECIAL COUNSEL
TO
DR. CONDOLEEZZA RICE
NATIONAL SECURITY ADVISOR (U)
Dated: June 7, 2002

(U) Subject: OSC File No. DI-02-0572
Vulnerabilities of the Department of Energy's Office of Transportation Safeguards (OTS)

(U) The concerns expressed in the allegations as to the security profile and potential vulnerabilities of the OTS appear to be based on information in excess of 5 years old. The issues presented can be derived from audits and reviews that were, and continue to be, conducted in order to determine the ability of the OTS to protect its cargo. The information learned from these audits was used to improve the security profile of the OTS, consequently much has changed. In addition to the changes resulting from these audits, OTS made changes during the Gulf War and following the events of September 11 to further enhance the security profile of its convoys. The following is the NNSA response to the issues:

DELETED

DELETED VERSION

U.S. Department of Energy Declassification Review	
1 st Review Date: 02/08/2005	Determination (Circle Number (s)) 1. Classification retained. 2. Classification change to: _____ 3. Contains No DOE Classified Info. 4. Coordinate with: _____
Authority: <input type="checkbox"/> AOC <input type="checkbox"/> DC <input checked="" type="checkbox"/> ADD Name: Michael L. Gates	
2 nd Review Date: 02/09/2005	5. Classification cancelled. 6. Classified Info. Bracketed 7. Other (Specify): _____
Authority: ADD Name: Charles L. Trujillo	

~~SECRET/NSI~~

DELETED

~~SECRET/NSI~~

DELETED

~~(S)~~ OSC Report: The staffing for convoys is set by the Director of TSS. The DOE operates under the Design Basis Threat to calculate, among other things, the protection necessary and delay mechanisms to use.

DELETED

a continuous process to review the threat against the TSS, and adjustments are made as required to address the threat. There is

(U) OSC Report: It is (redacted name) position that the danger to these convoys constitutes an immediate problem and that there is a need to recognize the significance of an attack on them.

(U) NNSA Response: The DOE/NNSA recognizes the significance of an attack on and/or the loss of NNSA control of nuclear weapons and special nuclear materials. In addition to the significant in-transit safeguards used to protect these materials, numerous other actions are taken to enhance their security. These include:

~~SECRET/NSI~~

- Limited distribution of information concerning the planning, routes, and execution of the shipments. The planning and scheduling of operational missions are carried out by "Q" cleared individuals who participate in the human reliability program to include polygraph testing. Information concerning operations is shared only on a strict need-to-know basis.
- Review by internal and external audit teams to include:
 - DOE Office of Independent Oversight and Performance Assessments/Office of Safeguards and Security Evaluations (FY-2001)
 - US General Accounting Office (FY-2002)
- Coordination with other NNSA, DOE, DoD, FBI, and other teams to identify changes in the threat and potential system vulnerabilities
- An ongoing process of upgrades and improvements to meet the changing characteristics and capabilities of potential adversaries

DOE/NNSA is serious about the protection of nuclear weapons and special nuclear materials while in transit. At every opportunity, improvements will be made to the OTS system to ensure the safe, secure transport of these materials.

~~SECRET/NSI~~

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