DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

SEP 26 2014

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M Street, N.W., Suite 218
Washington, DC 20036

Dear Ms. Lerner,

Thank you for your letter requesting an investigation of alleged security violations at the Naval Support Activity Bethesda (NSAB) and the Walter Reed National Military Medical Center (WRNMMC) (OSC DI-14-0535). The Secretary of Defense expressly authorized me to send this report on his behalf per 5 U.S.C. 1213 (d).

Enclosed is the report of the investigation led by the Naval Inspector General (NAVINSGEN) with the assistance of Commander, Navy Installations Command Inspector General (IG) and WRNMMC IG personnel. The investigation substantiated two allegations of unauthorized entry to NSAB and three allegations of unauthorized access to WRNMMC Information Technology systems by more than 20 contractor employees between September 2012 and November 2013. The investigation did not substantiate an allegation that a WRNMMC Information Technology government employee improperly granted Information Technology system access, because the individual did not have the authority to make that decision. Additionally, the investigation did not substantiate an allegation that a WRNMMC Information Technology government employee was also working for a WRNMMC Information Technology contractor while also serving as a government employee.

Based upon the findings of the NAVINSGEN report, the Secretary of the Navy is directing the Chief of Naval Operations to confirm full implementation of the NAVINSGEN's recommendations regarding NSAB; and, refer the NAVINSGEN report of investigation to the relevant organizational level for consideration and appropriate action, if any, to hold Department of the Navy individuals whom the report found to have been deficient in the performance of their duties accountable for such deficiencies.

I understand that you will provide this report to the Complainant, the President, and the House and Senate Armed Services Committees for their review. As has been the case with other reports submitted by the Department of Defense, I request that you exclude the names of witnesses in the public release of the report in accordance with the Freedom of Information Act, the Privacy Act, and Department of Defense policy. The Naval Inspector General will provide you a redacted copy of the investigation report for public release.

Again, thank you for bringing this matter to our attention. If I may be of further assistance, please let me know at your earliest convenience.

Sincerely,

Enclosure:
As stated

**Office of the Naval Inspector General**

**OSC DI-14-0535**
**NAVINSGEN 201401284**

**Report of Investigation**

ALLEGED SECURITY VIOLATIONS ALLOWING CONTRACTOR EMPLOYEES ACCESS TO SUPPORT ACTIVITY, BETHESDA AND GOVERNMENT NAVAL INFORMATION TECHNOLOGY SYSTEMS AT WALTER REED NATIONAL MILITARY MEDICAL CENTER, BETHESDA

24 SEPTEMBER 2014

*****

**Table of Contents**

**THIS PAGE LEFT BLANK TO FACILITATE 2 SIDED PRINTING**

# Office of the Naval Inspector General

## OSC DI-14-0535
## NAVINSGEN 201401284

## Report of Investigation

ALLEGED SECURITY VIOLATIONS ALLOWING CONTRACTORS ACCESS TO NAVAL SUPPORT ACTIVITY, BETHESDA AND GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS AT WALTER REED NATIONAL MILITARY MEDICAL CENTER, BETHESDA

24 SEPTEMBER 2014

*****

## Preliminary Statement

1. This report was prepared pursuant to an 11 February 2014 Office of Special Counsel (OSC) letter tasking the Secretary of Defense (SECDEF) to conduct an investigation under Title 5 United States Code Section 1213 (5 USC § 1213).[1]

2. OSC is an independent federal agency whose primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices. OSC also serves as a channel for federal workers to make allegations of: violations of law; gross mismanagement or waste of funds; abuse of authority; and a substantial and specific danger to the public health and safety.

3. Reports of investigations conducted pursuant to 5 USC § 1213 must include: (1) a summary of the information for which the investigation was initiated; (2) a description of the conduct of the investigation; (3) a summary of any evidence obtained from the investigation; (4) a listing of any violation or apparent violation of law, rule or regulation; and (5) a description of any action taken or planned as a result of the investigation, such as changes in agency rules, regulations or practices, the restoration of employment to an aggrieved employee, disciplinary action, and referral of evidence of criminal violations to the Attorney General.

[1] OSC copied the Inspector General of the Department of Defense (IG DoD), who is required to obtain an investigation of the allegations pursuant to Department of Defense Directive 5500.19, Cooperation with the United States Office of Special Counsel (OSC). The directive also requires the IG DoD and the DoD General Counsel to review 1213 investigations that must be personally reviewed by SECDEF or Deputy SECDEF.

**Information leading to the OSC Tasking**

4. The OSC tasking stems from a complaint alleging that employees of the Department of Defense (DoD) at Walter Reed National Military Medical Center (WRNMMC) and Naval Support Activity, Bethesda (NSAB) engaged in conduct that may constitute a violation of law, rule, or regulation, gross mismanagement, an abuse of authority, and a substantial danger to public safety. More specifically, the tasking letter states that the Complainant, Mr. Michael L. Robinson, a Personnel Security Specialist (PSS), who served as the Acting Command Security Manager (CSM) at the WRNMMC Personnel Security Office (PSO) disclosed that WRNMMC and employees in the Naval Support Activity, Bethesda (NSAB) Pass and ID office engaged in a number of serious management and safety breaches. These breaches, which resulted from not performing required background checks, allowed unvetted contractor employees to receive identity cards that permitted them to enter NASB and WRNMMC, and subsequently gain access to WRNMMC Information Technology (IT) systems. OSC stated Mr. Robinson, hereafter referred to as the "Complainant," consented to the release of his name.

5. The OSC tasking letter stated the following allegations are to be investigated:

> (1) That IT Department (ITD) contractor employees received U.S. Government identification (ID) badges and Walter Reed Base[2] access credentials without being subjected to a background investigation (BI);[3]
>
> (2) That ITD contractor employees have been granted access to Government IT systems, and sensitive[4] and classified

[2] Walter Reed, known as WRNMMC, is not a base; the base is NSAB on which WRNMMC is a tenant.

[3] Background Investigation (BI): "A personnel security investigation consisting of both record reviews and interviews with sources of information…covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday."

[4] Sensitive Information: Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DON payroll, finance, logistics, inventory, and

information,[5] prior to the initiation and conclusion of a BI and without being granted a security clearance (SC);

(3) That management has failed to take appropriate corrective actions to remedy these security shortcomings; and

(4) That at least one Government employee was simultaneously employed as both a GS-12 employee and as an ITD contractor employee for a contract that the employee managed, thus creating a conflict of interest within DoD.

6. The OSC tasking letter explained that the Complainant, who was responsible for managing the personnel and information security programs for WRNMMC, alleged that when he learned of the breaches by IT contractor employees, he informed both NASB and WRNMMC management officials, but they failed to take appropriate action to address the breaches. Consequently, the unvetted IT contractor employees continued to enter NSAB and WRNMMC, and continued to have access to WRNMMC IT systems containing Personally Identifiable Information (PII), and sensitive and/or classified information, even though these employees had never gone through a BI and SC.[6] The Complainant further alleged that at least one of the IT contractor employees was working as a contractor and a GS-12 ITD employee simultaneously creating a conflict of interest.

7. The OSC tasking letter provided additional information about Complainant's contentions, stating:

As part of his duties, Mr. Robinson is charged with identifying and addressing national security concerns and threats at Walter Reed. On 29 August 2013, Mr. Robinson

---

personnel management systems. Examples include FOUO, Unclassified Technical Data, State Sensitive but Unclassified (SBU), or Foreign Government information [DoD 5200.2-R]. **SECNAV M-5510.30**A defines a sensitive position as any position whose occupant could bring about, by virtue of the nature of the position, an adverse effect on national security. Noncritical Sensitive (NCS), the sensitivity level designated in the MedPro/B.E.A.T. contract is defined as having the potential for some to serious impact and/or damage.

[5] The contractor employees on the MedPro/B.E.A.T. contract did not have access to classified information. The WRNMMC ITD Chief confirmed no classified information was on the WRNMMC network. Additionally, MedPro/B.E.A.T. contractor employees did not have access to Critical Sensitive information; they only had access to non-critical sensitive information or, in the case of Kor Emp 1, non-sensitive information.

[6] Government refers to Federal Government.

became aware of the potential security breaches at Walter Reed when an [ITD] contractor employee, Kor Emp 1, entered the PSO with sensitive and personally identifiable information (PII) and inquired about the clearance and eligibility status of another [contractor] employee, Kor Emp 2.[7] Kor Emp 1 had been issued a Government identification badge and was wearing [a WRNMMC badge] when he arrived at the PSO. Based on the credentials Kor Emp 1 was wearing, Mr. Robinson believed that Kor Emp 1 had been properly vetted and cleared. However, through the course of their discussion, Kor Emp 1 revealed that he did not undergo a [BI] prior to employment and did not have a [SC]. Kor Emp 1 further admitted that he was able to bypass the PSO with the aid of Subject 1, the Walter Reed [ITD] Chief Operations Officer (COO). Mr. Robinson was able to confirm, via a review of information stored in the Joint Personnel Adjudication System (JPAS) that Kor Emp 1 had not been subjected to a prior BI and did not have the SC eligibility required for the position he held as a contract Program Manager (PM) within the [ITD].[8]

On 9 September 2013, Mr. Robinson notified Subject 1, a [NSAB] Base Police officer that Kor Emp 1 needed to be removed from the facility.[9] However, Mr. Robinson was later told by Subject 1 that the [NSAB] Base Police were instructed not to remove Kor Emp 1 or take any other action. Mr. Robinson stated that he asked who had directed them to refrain from further action, but Subject 1 would not provide him with this information. Mr. Robinson further explained that [NSAB] Base Access Control provided Mr. Robinson with documents that confirmed that Kor Emp 1 initially reported to [WRNMMC] on 4 December 2012, and that he had been working without a [BI] or a [SC] since that date.

Subject to limited exceptions, all Government employees, including contractors, must undergo a [BI] prior to appointment to any department or agency of the Government.

[7] WRNMMC PSO where the Complainant worked.

[8] The Joint Personnel Adjudication System (JPAS) is a Department of Defense (DoD) security clearance database system. JPAS is used as a forum to record and store personnel security clearance eligibility determinations and actions, as well as an individual's access to classified information.

[9] Subject 1 was at the time and remains a Security Specialist assigned as the NSAB Access Control Officer (ACO).

See Executive Order 10450, section 3(c).[10] Further, in addition to other requirements, an employee must have a favorable adjudication of a [BI] in order to be granted access to sensitive information. See Executive Order 12968, section 1.2(c). To implement these requirements at Walter Reed, DoD policy states that contractors must have a fully adjudicated clearance or favorable BI determination from a Central Adjudication Facility (CAF) prior to having access to IT Level I or Level II sensitive data. See Joint Task Force CapMed-I 5210.01 (Dec. 13, 2011). IT Level I designates a critical sensitive position in which there is a "potential for grave to exceptionally grave impact and/or damage," and an IT Level II designates a non-critical position, which has a "potential for some to serious impact and/or damage." See TASKORD Rl01210.01 (BRAC Transition Navy IT Access).[11] In addition, the Privacy Act of 1974 specifically states that all PII must be protected, and that agencies are responsible for establishing appropriate safeguards to protect such information. See 5 U.S.C. § 552a(e)(l0). An agency is in violation of the Privacy Act when it permits a contractor employee to have access to PII without a favorable [BI].

Mr. Robinson alleged that the above requirements have not been fully implemented at [WRNMMC]. Based on the conversations with his supervisor, Subject 2,[12] Human Resources Department Chief, and information stored in JPAS regarding Kor Emp 1, Mr. Robinson discovered that there are approximately 20 individuals who are employed as [ITD] contract employees who have not been subjected to a BI or been granted a [SC] to access sensitive and/or classified

[10] There is no Section 3(c) in the Executive Order; we understand the Tasker refers to Section 3(a). That section applies to civilian officers and employees of an Executive Department or Agency, but not to employees of contractors performing work under contracts.

[11] TASKORD R101201.01 (BRAC Transition Navy IT Access) dated 7 December 2010 signed by a former Commander, Joint Task Force National Capital Region, mandates personnel security requirements to assure ADP/IT-2 WRAMC personnel transitioning to WRNMMC have the proper Personnel Security Investigation (PSI) submitted for the designated ADP/IT level. The TASKORD requires NNMC to review the PSI and ensure submission of PSI documents to OPM before a temporary log-on will be granted and requires military, contractors, students and volunteers designated as Non-critical sensitive to have a NACLC or ANACI level of background investigation.

[12] Subject 2 is a Lieutenant Commander (LCDR) in the U.S. Navy (USN); we refer to him throughout this report by his military rank.

information. However, these individuals have received [WRNMMC] access credentials, and have positions in which they routinely have access to PII and Government information systems, which may contain sensitive and/or classified information.

Under the DoD policy, [SC]s and [BI]s for contract employees are submitted and maintained by the contract employee's Facility Security Office at their respective company. The [WRNMMC] PSO is not responsible for submitting or processing any requests for [SC]s or BIs for contract employees. If a contract employee is considered acceptable for employment based on a favorable eligibility determination via a CAF, they will be in-processed to [WRNMMC] by the PSO. The [NSAB] Base Police are charged with base access control and issuance of Government ID badges to all staff requiring access to [WRNMMC] facilities.

Mr. Robinson has alleged that through e-mail correspondence with Subject 1 regarding Kor Emp 1, he learned that Subject 1 and Subject 2 collaborated to enable ITD contract employees to deliberately bypass the above DoD policy requirements, and be issued Government ID badges and [WRNMMC] access credentials by [NSAB] Base Police. Due to the nature of the ITD contract employee positions; there is a possibility of exposure or compromise to sensitive and/or classified information, Government information systems, and PII.

After learning this information, Mr. Robinson, as Acting CSM, revoked the [SC]s of Subject 1 and Subject 2 and filed incident reports on both individuals to the DoD CAF. When Mr. Robinson filed the incident report on Subject 1, JPAS revealed that Subject 1 had both a Civilian and a Contractor Profile Sheet, indicating that Subject 1 was employed as both a DoD GS-12 civilian employee and as an ITD contract employee with SpecPro Technical Services. Based on this information in JPAS, Mr. Robinson further alleged that Subject 1's simultaneous employment as both a DoD GS-12 employee and a DoD contractor employee created a conflict of interest within DoD. In his position as [ITD] [COO], Subject 1 supervises the [ITD] contract employees.

8. The OSC letter further stated the Special Counsel concluded:

> . . . that there is a substantial likelihood that the information that the whistleblower provided to OSC discloses a violation of law, rule or regulation, gross mismanagement, an abuse of authority, and a substantial and specific danger to public safety.

**Summary of Conduct of the Investigation**

9. After receiving the OSC Tasking Letter, SECDEF initially forwarded it to the Secretary of the Navy (SECNAV), authorizing him to reply directly to OSC. SECNAV, in turn, tasked the Office of the Naval Inspector General (NAVINSGEN) to conduct an investigation and forward him the report for his action after review by the DON General Counsel.

10. NAVINSGEN, in turn directed the Commander, Navy Installations Command Inspector General (CNIC IG) to assist in the investigation because NSAB falls within the CNIC chain of command. The CNIC IG Investigating Officers (IOs) contacted the Complainant's attorney and arranged for an interview with the Complainant; IOs also contacted the WRNMMC IG, who formerly reported to the Navy's Bureau of Medicine IG, to arrange for access to WRNMMC personnel and documents.

11. The WRNMMC IG informed NAVINSGEN and CNIC IG that WRNMMC no longer reported to DON, but was instead a subordinate activity of the Defense Health Agency (DHA). After making preliminary inquiries, NAVINSGEN concluded that WRNMMC personnel had been transferred from DON to DoD by the time of the events described in the OSC Tasker and that WRNMMC was now part of DHA, which reports to the Under Secretary of Defense for Personnel and Readiness (USD (P&R)). In cooperation with the WRNMMC IG, the CNIC IG also determined that DON did not supply WRNMMC IT services or support at the time of the events described in the OSC Tasker.

12. After DHA agreed to conduct a joint investigation with DON and suggested NAVINSGEN take the lead, SECNAV requested SECDEF authorize a joint inquiry into actions by the two DoD Components that SECNAV would direct and oversee. Acting on behalf of SECDEF, the Deputy SECDEF (DEPSECDEF) authorized SECNAV to direct and oversee the investigation, which would be conducted by NAVINSGEN, CNIC IG, and WRNMMC IG. The written delegation of authority authorized the IOs full and unrestricted access to all DoD personnel and records they deemed pertinent to the inquiry. It required that SECNAV take actions pertinent to Navy activities and personnel described in the report; that USD (P&R)

take actions pertinent to WRNMMC and its personnel; and that DEPSECDEF send the report to OSC on SECDEF's behalf.

13. At the outset of the investigative effort, the CNIC IG IOs interviewed the Complainant, with his attorney present, by telephone. Information provided by the Complainant that was not contained in the OSC tasking letter appears in the findings of fact for each allegation as appropriate. During the course of their inquiry, the joint investigation team interviewed 31 witnesses by telephone or in person. They also reviewed 167 documents, including applicable instructions and regulations, contracts, personnel documents, incident reports, and e-mails.

14. NAVINSGEN submitted the report to the DON and DHA Offices of General Counsel before sending the report to SECNAV and USD (P&R) to review and act upon the recommendations, actions planned, and actions taken, to include personnel actions. Concurrently, as required by DoD Directive 5500.19, NAVINSGEN sent the report to the IG DoD and the DoD General Counsel for their review before forwarding the report to DEPSECDEF for final review, action, and transmission to OSC.

**Summary of Allegations and Conclusions**

15. Based on the contents of the OSC tasking letter and our preliminary review, we decided to write two allegations that address allowing contractor employees to enter NSAB and four allegations that address giving them access to the WRNMMC IT system. We also wrote one allegation to address the assertion that one WRNMMC IT government employee was also employed by an IT contractor working for WRNMMC.[13]

16. The NSAB access allegations are:

> Allegation One: That in December 2012, Subject 1, Access Control Officer, NSAB, failed to follow

[13] The four "allegations to be investigated" in the OSC tasking letter do not identify individual Subjects by name. Our past practice has been to write allegations naming specific individuals only when people are specifically identified in the OSC letter as those who engaged in wrongdoing. Thus, Allegation One identifies Subject 1 and Allegation Four identifies Subject 2 as Subjects. OSC did not name the person with the alleged conflict of interest, but we thought it necessary to identify Subject 1 in the allegation statement for Allegation Seven. We also named Subject 1 as the Subject of Allegation Five based on assertions in the OSC letter that he collaborated with Subject 2 to allow contractor employees access to IT systems. All of these names will be removed from the "public release" version of the report we provide OSC.

identity proofing and vetting requirements prior to allowing Kor Emp 1 access to NSAB, in violation of Section 1069 of the Fiscal Year 2008 National Defense Authorization Act (FY2008 NDAA) and its implementing regulations. **Substantiated**.

Allegation Two: That, between September 2012 and November 2013, NSAB failed to follow identity proofing and vetting requirements prior to allowing IT Department contractors access to NSAB, in violation of Section 1069 of the FY2008 NDAA and its implementing regulations. **Substantiated**.

17. We concluded allegation one was substantiated because Subject 1 acknowledged it was his duty to ensure that visitors to NSAB were properly vetted, to include running the visitor's name through the criminal justice information index maintained by the National Crime Information Center (NCIC), a component of the Federal Bureau of Investigation.[14] Although Subject 1 said the NSAB Pass and ID office that he supervised did not have a terminal that provided access to the NCIC index, he acknowledged that there was a terminal in another building on the installation that he or his subordinates could use to check the database. Subject 1 testified that he believed Kor Emp 1 was submitted for the required NCIC and Sex Offender Registry checks before NSAB Pass and ID office issued him his WRNMMC badge. However, when Subject 1 reviewed the NSAB NCIC log books on 7 August 2014, he could find no entry documenting a NCIC check on Kor Emp 1 on or about 4 December 2012 when he began work on the contract, and concluded the check was not performed at that time. Although Subject 1 did not vet Kor Emp 1 in December 2012, when his supervisors requested Subject 1 perform the appropriate checks on Kor Emp 1 in the Fall of 2013, the results were negative.

18. We concluded allegation two was substantiated because after we determined Subject 1 failed to ensure all of the other IT

[14] The NCIC index is a computerized index of criminal justice records that includes information about criminal history, fugitives, stolen property, and missing persons that is provided by the FBI, federal, state, local and foreign criminal justice agencies and authorized courts. It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year. The index also includes information about known or suspected terrorists and individuals who are required to register with a jurisdiction's sex offender registry. An individual who has access to the full range of indexes maintained by NCIC can satisfy all of the installation access requirements specified in various laws and regulations applicable to DoD by performing this one check.

contractor employees working with Kor Emp 1 were properly vetted, we then found that Subject 1's management chain failed to engage in the process and provide sufficient oversight to ensure the required checks were done by Subject 1 or his staff for all contractor employees. Specifically, neither the former nor the current NSAB CO ensured that the NSAB instruction and operating procedures specific to base access provided sufficient clarity to make certain that policy expressed in higher level guidance or instructions was implemented at the installation level. Also, when confronted with Complainant's concerns about Kor Emp 1 in the fall of 2013, while his superiors did ask Subject 1 to run the NCIC check on Kor Emp 1, they did not ask him to run the check on any of the other IT contractor employees, or at least ask Subject 1 to confirm that check was performed in December 2012 on all of the IT contractor employees about whom Complainant expressed concern. Had they done so, they would have learned that none had been vetted by NASB in December 2012.

19. The WRNMCC IT system access allegations are:

> Allegation Three: That, between September 2012 and November 2013, WRNMMC allowed IT Department contractor employees access to Government IT systems without first obtaining the results of a National Agency Check with Inquiries (NACI), in violation of the DoD policy established in 5200.2-R, DoD Personnel Security Program. **Substantiated**.
>
> Allegation Four: That, pending resolution of a contract dispute, Subject 2, Chief, Human Resources and Manpower, WRNMMC, failed to ensure personnel in the Personnel Security Office who reported to him initiated requests to OPM necessary for contractor employees to obtain the NACLC background investigation contemplated by the contract, before getting access to the WRNMMC IT network. **Substantiated**.
>
> Allegation Five: That, between September 2012 and November 2013, Subject 3, Chief Operations Officer, IT Department, WRNMMC, allowed Kor Emp 1 access to WRNMMC IT systems without first obtaining the results of a National Agency Check (NAC), in violation of DoD policy established in DoD 5200.2-R, DoD Personnel Security Program. **Not Substantiated**.

Allegation Six: That, from September 2012 to November 2013, WRNMMC failed to correct violations of DoD policy established in DoD 5200.2-R, DoD Personnel Security Program. **Substantiated**.

20. We concluded allegation three was substantiated because although DoD 5200.2-R required the contractor employees to have successfully completed a national agency check with inquiries (NACI) form of BI before getting access to the IT network, no one made the request to OPM necessary for that screening process to begin. The contract required the employees to undergo a national and local agency check with credit inquiries (NACLC), but that more extensive vetting process was not started because of a contract dispute that was never resolved. We used the NACI because it is required by the DoD instruction and felt it inappropriate to use the NACLC because that contract requirement was in dispute.

21. The failure to perform the NACI resulted from Complainant's refusal to initiate the requisite investigations as an alternative pending resolution of the contract dispute even though his supervisor requested he do so. We found that WRNMMC leadership tried to address the contract impasse as early as January 2013. The Deputy Commanding Officer for Administration agreed to pay the cost of the BIs, authorized Complainant's office, the PSO, to start the BI process, and assumed the risk of allowing contractor employees access to the WRNMMC IT network pending completion of the BIs, but neither the Complainant, nor anyone else, did them.

22. We did find that the subsequent contract for these IT services included the appropriate contract provisions; nonetheless, several of the contractor employees working under that contract have been allowed access to the WRNMMC IT network even though they have yet to complete the vetting process.

23. We concluded allegation four was substantiated because Subject 2, Complainant's first level supervisor, failed to take effective action to require Complainant or others in the PSO to initiate the screening process after the Deputy Commanding Officer for Administration authorized the PSO to start the process to obtain the NACLC form of BI contemplated by the contract pending resolution of the contract dispute.

24. We concluded allegation five was not substantiated because Subject 3 had no role in the decision to allow Kor Emp 1 access to the WRNMMC IT network. We used the NAC because this was the

BI required by the DoD instruction given the low level of access that Kor Emp 1 received in order to do his work.

25. We concluded allegation six was substantiated because the efforts WRNMMC leadership made to overcome the contract dispute and obtain a BI did not succeed at any time during the period of contract performance. The facts demonstrate that the contractor refused to take action to vet its employees because it believed the contract did not authorize and require such actions. The facts also demonstrate the Complainant refused to start the vetting process even though the Deputy Commander for Administration agreed that WRNMMC would bear the expense and authorized the PSO to undertake that effort.

26. Although WRNMMC expeditiously requested the Army contracting office amend the contract to require the contractor to vet its employees and Subject 2 requested the Complainant work with others at WRNMMC to get the vetting effort accomplished pending amendment of the contract, their efforts were unsuccessful. We substantiated the allegation because we believe WRNMMC (or the Army contracting office) should have directed the contractor to vet its employees and submit a claim, or, in the alternative should have directed Complainant or others working the PSO to start the process to vet those employees or face disciplinary action. We chose the DoD instruction as the standard because we thought it inappropriate to use the contract in light of the contract dispute.

27. The final allegation is:

> Allegation Seven: That Subject 3, Chief Operations Officer, IT Department, WRNMMC, was receiving compensation as a Government employee while concurrently receiving compensation from SpecPro Technical Services (STS), Limited Liability Corporation, to perform work that created a conflict of interest, from 6 December 2010 to 10 September 2013, in violation of conflict of interest provisions in 5 CFR § 2635, Standards of ethical conduct for employees of the executive branch. **Not Substantiated**.

28. We concluded allegation seven is not substantiated because we found no overlap between Subject 3's periods of employment or compensation. Subject 3 terminated his employment with STS on 5 December 2010 and began his civil service employment on 6 December 2010. We determined Complainant's belief that Subject 3's employment and compensation overlapped was the

result of an error in an authoritative government database that the Complainant consulted and that erroneously indicated Subject 3 did not terminate his employment with STS until September 2013.

## Background

### Description of NSAB

29. NSAB was established in conjunction with the 2005 Base Realignment and Closure Commission (BRAC) recommendation. NSAB is responsible for base operational support for its major tenant, the WRNMMC, and other tenant activities residing on the base to include: The Uniformed Services University of Health Sciences; the Armed Forces Radiobiology Research Institute; Commander, Joint Task Force (JTF) National Capital Region Medical Directorate (NCRMD) and several other key tenant commands that provide research, training, and support to the base population.

### September 2011 Merger of Army and Navy Medical Centers

30. As part of the 2005 BRAC, Walter Reed Army Medical Center (WRAMC) and National Naval Medical Center (NNMC) were merged to streamline the delivery of health services to military personnel and eligible patients in the National Capital Region (NCR). Effective 15 September 2011, WRAMC and NNMC merged and became WRNMMC. Of note, before the merger, the process for granting personnel access to the former WRAMC had been adjudicated at the local level without consulting any of the criminal or sex offender databases. The less stringent WRAMC adjudication requirements were not transferable to WRNMMC; they did not satisfy the more stringent personnel clearance requirements in place at NSAB and resulted in approximately 3,000 former WRAMC employees transferring to WRNMMC without having fully vetted background checks. WRNMMC permitted transferring WRAMC personnel, who did not have a background check, access to WRNMMC while aggressively working to complete background checks for transferring personnel that now required them.

31. Effective on 1 October 2013, DHA assumed responsibility for shared services, functions and activities of the Military Health System (MHS) and other common clinical and business processes. The DHA has authority over the multi-service markets, including the NCR. The JTF CAPMED Capital Medicine became the NCRMD, which now exercises authority, direction, and control over inpatient facilities and their subordinate clinics in the NCR.

The DHA is the immediate superior of the NCRMD, which directs WRNMMC and Fort Belvoir Community Hospital. These hospitals operate as joint facilities.

32. The merger of WRAMC and NNMC into a single larger organization with approximately 7,200 employees also resulted in extreme wait time to obtain essential service from the newly created WRNMMC ITD. The increased wait times negatively impacted the ability of WRNMMC to meet its mission.

33. During a Town Hall meeting in November 2012, the Commander, WRNMMC, discussed the issues related to the increased wait times for IT support and reported that approximately 20 additional contractor employees were being hired to increase the number of Support and Help Desk personnel.[15]

**Implementation of Base Access Vetting Requirements**

34. Enhanced installation access procedures for DoD and Navy installations have developed significantly since 27 August 2004, when President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." The Presidential Directive required the development and implementation of a mandatory government-wide standard for secure and reliable forms of identification for Federal employees and eligible contractors to gain physical access to federal installations and logical access to federal information systems. This standard identification, implemented by DoD as the Common Access Card (CAC), is required for federal employees and contractors who require routine access to federal facilities or federal information systems for more than six months. As implemented by the Office of Personnel Management, the DoD CAC and other Federal Personal Identity Verification (PIV) cards require at least a National Agency Criminal Check with Inquiries (NACI) to validate identity and ensure the individual's fitness and eligibility. Agencies must initiate the proper investigation and ensure completion of an FBI fingerprint check before issuing the card.

35. In January 2008, the President signed the National Defense Authorization Act for 2008 (FY08 NDAA) into law. By section 1069 of the FY08 NDAA, "Standards required for entry to military installations in United States," Congress directed the Secretary of Defense to develop access standards applicable to all

[15] JTF CAPMED is now the National Capital Region Medical Directorate (NCRMD). The heads of WRNMMC and NCRMD are now called "Directors."

military installations in the United States by July 1, 2008 and to implement them by 1 January 2009. At DoD's request, Congress later extended the deadlines to 1 February 2009 and 1 October 2010, respectively. The access standards were to include standards and procedures both for determining the fitness of individuals requesting access to military installations and for verifying their identities. The requirement imposed by section 1069 expanded upon the HSPD-12 mandate by requiring DoD access standards not only for federal employees and contractors, but for anyone requesting access to a military installation.

36. With Directive-Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," 8 December 2009,[16] DoD developed policy establishing the access standards and procedures mandated by section 1069 of the FY09 NDAA and directed DoD component heads, "to establish guidance and procedures to implement and comply with the policy contained in the DTM, as resources permit." The section 1069 access standards developed by DoD reiterated the CAC as the principle access card for physical and logical access to DoD installations and information systems in accordance with HSPD-12. The DTM also reiterated the identity proofing and fitness requirements established in accordance with HSPD-12 that require a minimum of a NACI investigation for any civilian or contractor issued a CAC. Under the DTM 09-012 policy, visitors, vendors and all other persons who do not possess a Federal Government or DoD-issued card must present an approved identity document, have a valid reason for entry and submit to specified criminal checks prior to being allowed unescorted access to a military installation. The minimum access standards developed by DoD specify that installation representatives must query the NCIC index, the Terrorist Screening Database and any other source determined by the DoD component or local commander prior to authorizing non-Federal Government and non-DoD-issued card holders' unescorted access to a DoD installation.

37. Specific provisions of Section 1069 and DTM 09-012 are included in the regulations section of allegation one, along with provisions of lower level implementing instructions.

[16] DTM 09-012 has been amended four times since 2009 to extend its expiration date. DTM 09-012 is currently scheduled to expire February 28, 2015. Its provisions have not yet been incorporated into DoD 5200.08-R or DoDI 5200.08 as anticipated.

**DoDIG NCACS Audit**

38. In September 2013, the IG DoD issued an audit report of NCACS, or RAPIDGate. The IG DOD auditors inquired into visitor access procedures at ten DON installations, including NSAB. They found that criminal background checks performed by the NCACS contractor using commercial, rather than government, databases were insufficient in that they allowed fifty-two felons to access Navy installations routinely before their felony convictions were discovered. The audit report stated that the felonies identified during the audit occurred an average of 13 years prior to passing the initial RAPIDGate screening. CNICINST 5530.2, however, identifies minimum standards for Navy installation commanding officers to consider for denying installation access that specifies felony convictions within the past 10 years. Accordingly, there is no requirement for Navy installations to conduct criminal background checks that exceed ten years. The DTM 09-012 is silent on this point. It does not specify the extent of the NCIC search to identify felony convictions in its minimum standards for vetting visitors.

39. The DoD auditors also found that seven of the ten Navy installations visited by IG DoD auditors lacked sufficient resources or capability to vet all contractors through the NCIC and Terrorist Screening Database as required by DTM 09-012. NSAB was one of the installations identified by the auditors that did not vet all contractors as required by DoD because its access control personnel did not have sufficient access to the NCIC index to perform the checks.

40. A significant finding in the report:

> Finding A. NCACS Did Not Effectively Mitigate Access Control Risks for Contractors Entering Navy Installations
>
> The Navy Commercial Access Control System, Rapidgate, did not effectively mitigate the access control risks of contractors accessing Navy installations. Specifically, numerous contractor employees enrolled in Rapidgate received interim installation access and Rapidgate credentials without having their identities vetted through mandatory authoritative databases, such as the National Crime Information Center (NCIC) database and the Terrorist Screening Database. Furthermore, as an alternative to NCACS, contractor employees could obtain a local daily pass without having their identities vetted through NCIC and the

Terrorist Screening Database. This occurred because—in an attempt to reduce access control costs—CNIC did not:

- follow Federal credentialing standards and DoD contractor vetting requirements and

- provide 7 of the 10 installations visited with the appropriate resources and capabilities to conduct required contractor background checks.

As a result, 52 convicted felons received routine, unauthorized access to Navy installations for 62 to 1,035 days since Eid Passport's initial public record checks did not identify the felony convictions. This placed military personnel, dependents, civilians, and installations at an increased security risk.

41. In July 2014, IG DoD initiated a follow-up review of the seven Navy installations to determine whether the installations previously visited had resolved their respective issues for accessing the NCIC index and Terrorist Screening Database and were now conducting required checks of contractor personnel enrolled in the NCACS before issuing installation passes. The review will also determine what actions the installations have taken to correct the deficiencies IG DoD noted in the original audit. As part of this effort, IG DoD audit personnel visited the NSAB Pass and ID office the week of 25 August 2014 to perform a follow-up of NSAB efforts to implement Finding A recommendations. The auditors have not completed their analysis of NSAB and anticipate that a final report will be published around the beginning of CY 2015.

**NAVINSGEN Review of Installation Access Controls**

42. Since September 2013, the Office of the Naval Inspector General (NAVINSGEN) has made implementation of installation access controls an area of special focus during its command inspections and area visits. NAVINSGEN observations are consistent with the findings of the September 2013 IG DoD NCACS audit report. In general, however, NAVINSGEN has found that installation commanders are making the best efforts they can to allocate limited resources in such a way as to comply with the intent of the access control program. NAVINSGEN inspections have not identified any instance where the failure to screen a visitor in the manner contemplated by DoD or Navy regulations has created a specific danger to public health and safety. NAVINSGEN further recognizes that IG DoD is currently engaged in

a follow-up audit to verify Navy corrective actions associated with the September 2013 IG DoD NCACS audit report have been implemented and are effective.

**Complainant's Previous Inquiries**

43. In May 2013, the Complainant sent the WRNMMC Chief of Staff (COS) an e-mail with the subject, National Security Concerns. In the e-mail the Complainant stated that the command faced "imminent threats and security concerns that potentially place patients, staff, visitors, and the facility at risk." The Complainant did not specify what the threats were.

44. On 10 September 2013, the Complainant filed an incident report on Subject 3 with the DoD Central Adjudication Facility (CAF) and alleged Subject 3 had allowed illegal or unauthorized entry to the command's Government technology systems or components. The Complainant alleged Subject 3 had openly authorized non-vetted, contractor employees access to ADP I - Critical Sensitive, and ADP II - Non-Critical sensitive, systems, networks, and information. The Complainant further alleged that Subject 3 had entrusted the same unauthorized, non-vetted, contractor employees with handling sensitive information and/or PII protected under the Privacy Act of 1974.[17]

45. On 23 September 2013, the Complainant raised base access security concerns, similar to those raised in this OSC complaint, to the SECDEF. SECDEF forwarded that prior complaint (OSD011554-13) to the DHA NCRMD. The subject of the tasker was: REQUEST FOR IMPARTIAL REVIEW OF THE BASE ACCESS SECURITY PROTOCOL AT THE WALTER REED NATIONAL MILITARY MEDICAL CENTER. The 23 September 2013 complaint alleged the protocol used by NSAB to issue badges was flawed. The Complainant alleged NSAB base police and ITD leadership had been ignoring security concerns, the security vetting process for employment at WRNMMC was not receiving the necessary support, and WRNMMC ITD leadership disregarded DoD Information Security policy and had given DoD IT systems' access and administrative rights to a number of contractors who had not been properly vetted or cleared.

46. On 1 October 2013, the Director, DHA NCRMD, tasked the complaint to the Director, WRNMMC; requested a response for the USD (P&R) no later than 18 October 2013; and forwarded the

[17] Automated Data Processing

complaint concerning NSAB to the CO, NSAB, and Commandant, Naval District Washington (NDW), for review.

47. On 3 October 2013, the Complainant filed an incident report on Subject 2 with the DoD CAF in which he alleged Subject 2 had supported and condoned a process to deliberately bypass the command's personnel security staff and protocol by allowing contractor employees in IT designated sensitive positions to in-process and be issued Government IDs and credentials for accessing the facility, in addition, to gaining access and administrative rights and privileges to Government IT Systems without the appropriate BI, determined eligibility, or approved access. The incident report resulted in suspension of Subject 2's clearance.[18]

48. On 7 October 2013, the Complainant testified to having contacted the Federal Bureau of Investigation (FBI). The Complainant reported to FBI Specialist 519 that activities associated with the command threatened National Security and placed its patrons, staff, and the facility at risk; he had been unable to get this message across to leadership; loop holes and resistance allowed non-vetted employees and contractors to in-process, receive credentials, and access sensitive information prior to having been deemed eligible by the U.S. Government; and these security concerns were more concerning than those associated with the Navy Yard Shooting. The Complainant stated that Specialist 519 advised the Complainant that she would pass the information to an FBI Agent, who would follow up if the concerns were in the FBI's interest.

49. On 9 October 2013, the current CO, NSAB, submitted an "Info Memo," SUBJECT: Walter Reed National Military Medical Center (WRNMMC) & Naval Support Activity Bethesda (NSAB) Security Concerns, to the Commandant, NDW, Copy to the Chief of Staff and Deputy Commandant, NDW, and the Executive Director, NSAB (NSAB ED). The memo was prepared in response to a 1 October 2013 e-mail from the Director, NCRMD, in which she requested NDW provide input to include in her response to SECDEF. The current CO, NSAB states in the memo that the Complainant referenced concerns with the procedure NSAB utilized to issue employee ID badges for access to the installation, as well as Security Clearance and Information Security Policies within WRNMMC's IT and HR Departments. The current CO, NSAB stated the Info Memo addressed the Complainant's access control concern at NSAB only. The current CO, NSAB cited to the following references:

[18] Subject 2 testified that DON CAF reactivated his clearance on 6 March 2014.

(a) NSABETHINST 5530.2 (Access Control Procedures);

(b) DTM-09-012 (Interim Policy Guidance for DoD Physical Access Control);

(c) OPNAVINST 5530.14E (Navy Physical Security and Law Enforcement Program); and,

(d) CNICINST 5530.14A (Ashore Protection Program).

50. The current CO, NSAB stated in the memo that reference (a), NSAB's local Access Control instruction, was developed in accordance with references (b) and (c); per reference (d), NSAB's access control procedures contain identity proofing and vetting measures to determine the fitness of an individual requesting and/or requiring access prior to the issuance of a local access credential or pass. The current CO, NSAB further stated in the memo:

> An ID Card application is forwarded to the NSAB Access Control Officer by the sponsoring department or tenant. This application includes the purpose and duration of the visit and is signed by the sponsoring Department Head.
>
> The individual requesting unescorted access presents a valid form of Federal or state government identification as prescribed in references (b) and (d).
>
> The individual is subjected to criminal history and Sex Offender Registration and Notification Act (SORNA) checks through the Maryland Electronic Telecommunications Enforcement Resource System/National Crime Information Center (METERS/NCIC) and through the Navy's Consolidated Law Enforcement Operations Center (CLEOC) to determine fitness of the individual and ensure they are not currently barred from a Navy installation.
>
> Adverse information uncovered during the check is evaluated by the Security Director and a recommendation to deny or grant access is made to the NSAB Commanding Officer.
>
> If granted access, an ID card is issued for the duration of the visit or one year. Long term employees ID cards must

> be renewed annually in conjunction with an annual re-verification METERS, NCIC, and CLEOC checks."[19]

51. On 15 October 2013, the Complainant provided additional information to DoD CAF stating Subject 1 was working as a DoD civilian overseeing and/or supervising an ITD contract billed to the Government while working on the same contract as a contractor employee thus establishing a conflict of interest.[20] The Complainant stated WRNMMC PSO had not been afforded direct access to the CO, WRNMMC, to ensure effective management of the Command's security program as regulated in the SECNAV M-5510.30, Department of the Navy Personnel Security Program, and that the Complainant had notified the COS, WRNMMC; FBI; and, SECDEF of the security concerns.

52. On 18 October 2013, DoD CAF requested additional information, which the Complainant provided on 21 October 2013. The complainant stated Subject 1 was still employed at WRNMMC; that approximately 20 individuals had unauthorized access to sensitive systems; that the WRNMMC PSO had no way of determining if classified information was compromised; and, the command had not taken any disciplinary action against Subject 1 as a result of the security incident. The incident report the Complainant filed on Subject 1 with DoD CAF resulted in suspension of Subject 1's clearance.[21]

53. On 23 October 2013, the Director, WRNMMC responded to the Complainant's 23 September 2013 with a memorandum for SECDEF and stated:

> WRNMMC is in compliance with DoDINST 5200.2R and SECNAVINST 5510.30 in regards to personnel security and temporary access.

54. In his letter, the Director, WRNMMC also said the Civilian Human Relations Center and Labor Management and Employee

---

[19] The current CO, NSAB's "info memo" explains the process required in the noted instructions; he does not state NSAB is in compliance with the process as described. Investigators contacted numerous individuals at NDW and NSAB who were identified in e-mails as having received the current CO, NSAB's memo to determine whether NDW provided input for use in the Director, WRNMMC's response to SECDEF. We were unsuccessful in our efforts to find any evidence to show that NDW took this for action or submitted a response to the Director, NCRMD's request for information about the Complainant's concerns regarding NSAB access.

[20] The same allegation is addressed in Allegation Seven of this report.

[21] Subject 1 testified that DON CAF reactivated his clearance on 6 March 2014.

Relations staff, as part of the National Capital Region Medical Directorate (NCR MEDDIR), provided employee support to WRNMMC and was granted access to IT systems within WRNMMC in accordance with DoD 5200.2R and SECNAVINST 5510.30. The Director, WRNMMC's 23 October 2013 letter to SECDEF further stated that the ITD contract-related concern referenced in the letter of 23 September 2013 "will be" in compliance with DoD 5200.2R and SECNAV Instruction 5510.30 as of 27 November 2013.[22] The Director stated the contract referenced in the letter was awarded in November 2012 and that in January 2013, WRNMMC discovered the incumbent contract was awarded without the requirement for contractor employees to have any background investigation or security clearance. The Director stated the contract was then amended via the regional contract authorities to include the background check requirements; the vendor did not possess the resources to meet the need, leaving four staff noncompliant in the background investigation requirement; and, at that time, there were five months remaining on the contract.[23] The Director stated leadership made the decision to continue utilizing the four critical resources, but limited their permissions and work scope.[24] The Director, WRNMMC stated the staff did not have access to classified material and were supervised by credentialed/cleared supervisors."[25]

## Summary of Evidence Obtained During Investigation

### Allegation One

That in December 2012, Subject 1, Access Control Officer, NSAB, failed to follow identity proofing and vetting requirements prior to allowing Kor Emp 1

[22] The subsequent IT contract with STS awarded on 13 November 2013 did not contain language requiring the contractor to conduct the background checks. However, the contract included language requiring the contractors to have a SECRET clearance at the beginning performance of the contract.

[23] Investigators determined the WRNMMC ITD discovered NARCO amended the September 2012 to November 2013 IT contract to include modified position hours and the deletion of the Ticket Systems Administrator position, but failed to include the specific language regarding background checks.

[24] Witnesses who contributed to efforts to prepare WRNMMC's response to SECDEF were not able to identify the four contractor employees mentioned in the Director, WRNMMC's letter.

[25] The investigators noted several inconsistencies in the Director, WRNMMC's memo. The Director stated WRNMMC complied with the standards then contradicted this assertion when he stated that as of 27 November 2013 WRNMMC would be in compliance. None of the witnesses interviewed could provide the names of the four "critical resources" the Director referenced in the memo.

access to NSAB, in violation of Section 1069 of the Fiscal Year 2008 National Defense Authorization Act (FY2008 NDAA) and its implementing regulations.

**Findings of Fact**

55. The Complainant testified that one of his primary responsibilities as the PSS entailed identifying and addressing national security concerns and threats at WRNMMC. The Complainant stated that he became aware of potential security breaches at WRNMMC on 29 August 2013 when Kor Emp 1, an ITD contractor employee, entered the PSO to inquire into the SC and eligibility status of a fellow contractor employee, Kor Emp 2. During the course of their discussion, the Complainant noted that Kor Emp 1 had in his possession sensitive information and PII.

56. The Complainant stated that Kor Emp 1 possessed a Government ID badge and was also wearing a WRNMMC badge, leading him to believe Kor Emp 1 had been properly vetted and cleared. However, during the course of their discussion, Kor Emp 1 revealed that he had not undergone a BI nor had he been issued a SC prior to his employment with the WRNMMC ITD on contract number W91YTZ-12C-0157.

57. The Complainant testified that Kor Emp 1 further admitted he had “bypassed the PSO” with the assistance of Subject 1. Following this disclosure, the Complainant queried JPAS and confirmed that Kor Emp 1 had not undergone a prior BI nor did he hold the SC eligibility required to serve as a contractor’s PM in the WRNMCC ITD.

58. On 9 September 2013, the Complainant testified that he informed Subject 1 that Kor Emp 1 needed to be removed from the WRNMMC facility. Sometime after, the Complainant alleged Subject 1 informed him that NSAB police officers had been instructed not to remove Kor Emp 1 from WRNMMC or to take any further action regarding this matter. The Complainant further alleged that Subject 1 declined to disclose who had instructed the police officers not to take further action.

59. On 11 September 2013, the Complainant stated that the NSAB Pass and ID Office provided him with documentation confirming that Kor Emp 1 reported aboard WRNMMC on 4 December 2012 and that he had been working in the facility’s ITD without a completed BI/SC since that date.

60. The Deputy Chief Information Officer (CIO), ITD, WRNMMC (WRNMMC CIO/COR) testified he was the Contracting Officer Representative (COR) and Kor Emp 1 was the Program Manager on the MedPro/B.E.A.T. contract. When Kor Emp 1 came on board in December 2012, the WRNMMC CIO/COR confirmed he escorted him during part of the command's check-in process. The WRNMMC CIO/COR described the form used for in-processing, which was signed by the department head, and explained that Security also was required to sign the form. The WRNMMC CIO/COR testified he believed that the staff in the Pass and ID Office most likely conducted "a very generic background check," which he described as looking to see if there were any warrants out on Kor Emp 1. After the check was completed, they issued Kor Emp 1 a staff badge.

61. On 29 July 2014, investigators contacted Kor Emp 1 in hopes of obtaining his first-hand perspective of the events that transpired. However, Kor Emp 1, who is no longer a contractor employee working on contract number W91YTZ-12C-0157 at WRNMMC, declined to participate in this investigation.

62. Subject 1's immediate supervisor, Deputy Security Director, NSAB, acknowledged he allowed Subject 1 to "run the access process" at WRNMMC.[26] Subject 1's supervisor stated contractors gained access to the facility if they came through RAPIDGate and were issued an ID card or if the CO authorized and issued them a WRNMMC badge. Subject 1's supervisor confirmed that Kor Emp 1 received a WRNMMC badge in December 2012, but the Complainant expressed concern about whether Kor Emp 1 should have been granted the badge. Subject 1's supervisor recalled that in September 2013, Subject 1 checked in the system and determined Kor Emp 1 could have base access because he was not a registered sex offender, he did not have any criminal history in NCIC, and he passed the local check they conducted on him through CLEOC.

63. The Director, NSAB Security Operations (NSAB DSO)), Subject 1's second-level supervisor, stated that WRNMMC contractor employees were required to have one of the following: a RAPIDGate ID card issued through the Navy Commercial Access Control System (NCACS); a day pass if they did not have a NCACS ID; or a local WRNMMC badge.[27]

---

[26] To minimize the possibility that the reader might confuse Subject 1's immediate supervisor, with the Complainant, we refer to him in this report as "Subject 1's supervisor."

[27] On 19 June 2014, an NDW Headquarters representative confirmed Kor Emp 1 was not issued a RAPIDGate ID.

64. The NSAB DSO also stated they followed NSABETHINST 5530.2, Enclosure 4, when issuing a badge to a contractor employee. He explained that the contractor employee was required to have a memorandum signed by their department chief in order to receive an individual badge and a vehicle pass for driving and parking aboard the installation. Following receipt of the signed memorandum, personnel from the NSAB Pass and ID Office would run the applicant's name through the NCIC index and the Sex Offender Registry to determine any past criminal history. If the individual was cleared through these background checks, he or she would be issued a WRNMMC badge. The NSAB DSO also stated that the process of issuing badges was not documented in writing, however, Subject 1 had been tasked with drafting an instruction and they have had Standard Operating Procedures (SOPs) in place for base access control.

65. The NSAB DSO further stated he confirmed Kor Emp 1 was issued a badge in December 2012, but that he (the NSAB DSO) was not working in Security Operations at the time. The NSAB DSO recalled instructing Subject 1 to check Kor Emp 1 twice in NCIC and on both occasions the results came back without any derogatory information about him.[28] The NSAB DSO further said he discussed this situation with the NSAB Executive Director, NSAB (NSAB ED), who contacted the ITD. The NSAB DSO stated the ITD Head,[29] whose name he could not recall, was the one who discussed the situation regarding Kor Emp 1 with the NSAB ED and requested they not revoke Kor Emp 1's access to the installation. The NSAB DSO confirmed that he relayed the NSAB ED's decision not to revoke Kor Emp 1's access to WRNMMC and to Subject 1. The NSAB DSO further testified that the Complainant never explained to him or his staff what the issue was that required them to revoke Kor Emp 1's base access.

66. The NSAB DSO testified that CNICINST 5530.14A, dated 29 May 2013, Chapter 12, addressed how contractor employees were to be processed through Access Control, and that this document "drove them to NCACS." The NSAB DSO stated that contractors were then issued either a RAPIDGate ID card or a one day base pass. The NSAB DSO further testified that he doubted that the process for vetting contractors, as outlined in NSABETHINST 5530.2, had ever been followed the way it was written in the instruction.

[28] The IOs determined Subject 1 conducted the NCIC check in September 2013 after the Complainant brought this matter to the NSAB DSO' attention and not in 2012 when Kor Emp 1 received his badge.
[29] The WRNMMC ITD Chief

67. The NSAB ED stated that he was first made aware of the situation involving Kor Emp 1 and the badge that he had been issued in September 2013. During his testimony, the NSAB ED referred to an email message dated 9 September 2013 and stated he believed this to be an IT matter rather than an issue with Kor Emp 1's WRNMMC badge granting him access to the base.

68. The NSAB ED stated that he consulted the WRNMMC CIO/COR, who informed him that he needed Kor Emp 1, as he was considered critical to the contract.[30] The NSAB ED also stated that the WRNMMC CIO/COR never indicated he had any concerns about Kor Emp 1 being on the base, and confirmed no one had initiated Kor Emp 1's background check to date, and that Kor Emp 1 did not have a secret clearance in JPAS. The NSAB ED further testified that the WRNMMC CIO/COR informed him the wording in the contract neglected to state whether or not these contractor employees required a background check.

69. The NSAB ED testified it was his decision to allow Kor Emp 1 to maintain his access to the installation, it was within his authority to do so, and he did not consult the NSAB CO before making his decision. The NSAB ED stated that he relayed his decision to the NSAB DSO, who informed Subject 1 there was no reason to revoke Kor Emp 1's base access.

70. The NSAB ED testified that Kor Emp 1 was a contractor employee at WRNMMC who had been issued a badge granting him (SubK Emp1) access to NSAB in December 2012. The NSAB ED also confirmed that Kor Emp 1 did not have a completed background investigation or secret clearance on file at the time he was granted base access. The NSAB ED further stated that he was aware NSAB was not following the instruction on issuing badges properly, but stated they would begin to adhere to it on 1 October 2014. The NSAB ED stated the current policy regarding badge issuance was not in writing but that they followed more of "a word of mouth" policy with the medical center. According to The NSAB ED, the Joint Commission, an independent, not-for-profit organization that accredits hospitals and other health care facilities, required NSAB to issue badges granting access to WRNMMC. The NSAB ED also stated that it was not necessary to have a CAC in order to be issued a WRNMMC badge.

71. The former Commanding Officer (CO), NSAB, who served as the CO, NSAB, during the period October 2011 through early September 2013, testified that he interpreted NSABETHINST 5530.2 4d (4)(e)

[30] The WRNMMC CIO/COR was also the COR for the MedPro/B.E.A.T. contract during the period in question.

to mean a contractor employee was not required to have a CAC in order to be issued a WRNMMC badge. He also stated that no one had ever approached him with any concerns or complaints regarding the language in NSABETHINST 5530.2 and that he was not aware of anyone deviating from the process outlined in the instruction. The former CO, NSAB further testified that Subject Matter Experts reviewed WRNMMC base access control procedures while he was CO and never raised any concerns. The former CO, NSAB stated that although he did not know the exact process that was used at the time Kor Emp 1 was issued his badge, he believed the NSAB's Security Office followed the process outlined in NSABETHINST 5530.2 in order to provide him what was required for a contractor employee. The former CO, NSAB stated, "If the Medical Center said give him a badge, we issued a badge." In his testimony, the former CO, NSAB clarified that contractor employees received either a WRNMMC badge or a NCACS badge, and that he was not responsible for issuing CACs since it was the Personnel Support Detachment's (PSD's) responsibility to issue CACs to individuals who required logical (computer) access. The former CO, NSAB further stated that he relied on Subject 1 and his office to handle processing contractor employees and issuing them the appropriate ID to access NSAB.

72. In his testimony, the current CO, NSAB, confirmed NSAB's Pass and ID Office is responsible for issuing badges for individuals requiring access to WRNMMC. The current CO, NSAB referenced an information memorandum dated 2 October 2013 that he wrote in response to the Complainant's 23 September 2013 letter to SECDEF regarding security concerns pertaining to WRNMMC and NSAB.

73. In his testimony, The current CO, NSAB stated that the information memorandum he prepared only addressed the Complainant's concern regarding access control at NSAB and the procedures NSAB followed in order to issue employee ID badges for access to the installation; it did not address the Complainant's additional concerns regarding SCs and information security policies within WRNMMC's IT and HR Departments.

74. In his testimony, the current CO, NSAB provided further insight regarding the contents of the information memorandum dated 2 October 2013. The current CO, NSAB cited Reference A, NSABETHINST 5530.2, "Access Control Procedures," as the local access control instruction NSAB followed in addition to two other references, DTM-09-012 "Interim Policy Guidance for DoD Physical Access Control," and OPNAVINST 5530.14E, "Navy Physical Security and Law Enforcement Program." In addition to these

references, the information memorandum addressed provisions specified in CNICINST 5530.14A, “Ashore Protection Program.” Specifically, that NSAB’s access control procedures contained identity proofing and vetting measures to determine the fitness of an individual requesting and/or requiring access prior to the issuance of a local access credential or pass. The current CO, NSAB further stated that the procedure required the sponsoring department to forward an ID Card application to the NSAB ACO.

75. The current CO, NSAB testified that the ID Card application included the purpose and duration of the visit and the Department Head’s signature. The current CO, NSAB stated the individual requesting unescorted access then presented a valid form of a Federal or state Government ID, followed by the NSAB Pass and ID Office check of his/her criminal history and Sex Offender Registration and Notification Act (SORNA) through the Maryland Electronic Telecommunications Enforcement Resource System/National Crime Information Center (METERS/NCIC) and through the Navy’s Consolidated Law Enforcement Operations Center (CLEOC) to determine the individual’s fitness and ensure that he/she was not currently barred from a Navy installation. The current CO, NSAB testified that if the contractor employee was granted access, NSAB issued the individual an ID for the duration of the visit or one year but, if NSAB uncovered adverse information about the individual during the check, the Security Director conducted an evaluation and made a recommendation to the NSAB CO regarding whether or not to deny or grant access to the individual.

76. On 29 August 2011, Subject 1 was hired as a Security Specialist to fill Agency Position Number A063A-1038553. Subject 1 testified that he was a Security Specialist assigned as the NSAB ACO in charge of the NSAB Pass and ID Office, and that the base access control process was one of his responsibilities. Subject 1’s Position Description (PD), dated 3 May 2011 states:

> The Access Control Program Manager [also referred to as the ACO] is responsible for providing expert analysis and highly specialized services relating to access control programs and measures for the Naval Support Activity Bethesda [NSAB], tenant commands and activities, as well as management of the Pass and ID Office, serving as the installation Parking Coordinator, and Navy Contractor Verification System Trusted Agent Security Manager (CVS TASM). The function of this position is to provide for management of the installation access control measures such

as access control programs, issuance of hospital identification cards, registration of privately owned vehicles, issuance of parking permits, and the qualification and authorization for personnel to enter the installation."

77. Subject 1's PD, Major Duties, paragraph 2c states:

The incumbent will plan, schedule, and conduct activities to evaluate and recommend ways to improve the effectiveness and efficiency of program-related policies, post orders, and standard operating procedures to improve the effectiveness and efficiency of the program and overall physical security of the Naval Support Activity Bethesda and program or project operations."

78. Subject 1's PD, Major Duties, paragraph 2g states:

Manage the receipt of, conducting of criminal history background checks for all prospective civil service employees, contractors, vendors, and long-term visitors to the installation. Manages the completion of periodic criminal history background checks on civil service, contractor personnel, and vendors, in accordance with established policies. Approves or disapproves these personnel for access to the installation based on the results of their criminal history background. Utilize the Federal Bureau of Investigation (FBI)'s National Crime Information Center (NCIC) and the State of Maryland Criminal Justice Information System (CJIS). Utilize expert analysis in determining the approval or disapproval of persons for access to the [NSAB] installation."

79. Subject 1's PD, Major Duties, paragraph 3 states:

The incumbent will be thoroughly familiar with the requirements to safeguard the [NSAB] installation against access by unauthorized persons, and persons who are not qualified to enter a Department of Defense installation. The incumbent shall be highly knowledgeable of DoD and DON physical security instructions, policies and related guidance necessary to establish compliance with DON requirements."

80. NSABETHINST 5530.2 describes the duties of Pass and ID personnel in paragraph 4.f. which states:

> f. Pass and ID Personnel. Pass and ID personnel will be the subject matter experts on all Pass and ID issues. Personnel will conduct themselves in a professional and courteous manner at all times, remain up to date with all Instructions, Post Orders, procedures, security directive and command instructions."

81. We conducted three separate interviews with Subject 1 in order to reconcile the various discrepancies in his testimony concerning his understanding of the applicable regulations, his knowledge of the access control process for contractor employees, and the specific circumstances regarding Kor Emp 1 receiving access to the installation. The paragraphs that follow contain information he provided to us in each of his interviews and several follow-up emails.

82. In his initial interview, Subject 1 described the process by which a contractor employee obtained a badge to access WRNMMC in December 2012, the time when Kor Emp 1 began working as a contractor employee in the WRNMMC ITD. According to Subject 1, contractor employees checked in with their office of assignment and obtained a signed Memorandum for Renewal of WRNMMC and/or Vehicle Decals from their Department Head. After obtaining a United States Department of Defense Military Health System (DMHRSI) stamp on the signed memorandum from the Department Head, the contractor employee then proceeded to the NSAB Pass and ID Office for further processing. Subject 1 stated that contractor employees were required to fill out NSABETHINST 5530.2 enclosure 4, NSAB's ID Card and Vehicle Pass Application, enclosure 5, Memorandum for Renewal of WRNMMC ID Badge and/or Vehicle Pass, a Privacy Act Statement, and present two different forms of ID. Subject 1 explained that NSAB Pass and ID would conduct a criminal history background check through the NCIC, a sex offender registry check, and a CLEOC check to ensure that the individual was not debarred from any Navy or Marine Corps installations. Subject 1 further explained that during the time Kor Emp 1 checked in, applicant's names were submitted ahead of time due to the fact that they did not have an NCIC terminal in the NSAB Pass and ID office. Accordingly, Subject 1 testified that he or one of his assistants would have to go to Dispatch, which was located in another building, to run the NCIC check then log the query in the log book. NSAB personnel would then review all presented documents prior to issuing the individual a WRNMMC badge.

83. Subject 1 initially stated that in December 2012 NSAB did not have the resources and/or capabilities in the NSAB Pass and

ID office to conduct NCIC checks. He further stated there was only one terminal on the installation in December 2012, but that it was located in Dispatch. Accordingly, a staff member in the Security Department conducted a background check of each contractor employee's criminal history to be certain that he/she did not have any felony convictions. This check was then documented in the NSAB Pass and ID Office's records, and the contractor employee was issued a badge (often referred to as a Walter Reed badge) permitting access to the base. In a follow up email message dated 6 August 2014, Subject 1 clarified this aspect of testimony by stating that he misspoke during his interview. According to Subject 1, NSAB in fact did have NCIC access in 2012, however, they only had one terminal installed at the time, which was located in the Dispatch office. Subject 1 also mentioned in an email message dated 7 August 2014, that during a separate larger-scale DoD IG report released in 2013, it was determined that NSAB lacked sufficient resources to conduct NCIC checks.

84. The investigators obtained and reviewed a copy of the report Subject 1 referenced in his email message dated 7 August 2014. The DoD IG report, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," dated 16 September 2013. The report included an examination of NSAB access controls and found NSAB did not provide installation personnel with the appropriate resources to vet all contractors because it lacked sufficient resources (terminals) to access the NCIC and Terrorist Screening databases. The report also identified problems with the use of NCACS.

85. According to Subject 1, during the time period of 1 October 2011 and 30 September 2013, the former CO, NSAB, directed him to follow the existing instructions until they were superseded and that he followed the former CO, NSAB's direction. Subject 1 stated that on 4 December 2012, when the Pass and ID office issued Kor Emp 1 a WRNMMC ID badge, NSAB followed the Joint Commission requirement pertaining to ID badges dated 13 January 2009; National Naval Medical Center Instruction (NATNAVMEDCENINST) 5527.1 "Criminal Background Investigation Standards and Requirements for Contractual Employment On Board National Naval Medical Center (NNMC), dated 8 August 2009; and NSABETHINST 5530.2, "Access Control Procedures," dated 15 December 2011.

86. Subject 1 stated that the Joint Commission, dated 13 January 2009, required the facility to comply with regulations

issued by the state of Maryland. The Joint Commission requirement states:

> The standards require that the organization identifies individuals entering its facilities. The organization is expected to determine who requires identification and how the process is implemented. If the policy requires all staff to wear ID staff badges, then all staff (including Physicians) would need to comply. Photo IDs, name on badges (first, last, both, one or the other, etc.) may be necessary as some states have specific standards. Check with the local Authority Having Jurisdiction for additional guidance."

87. Subject 1 stated that NSABETHINST 5530.2 contained problematic language, specifically the wording in paragraph 4d(4)(e), regarding whether or not contractors were required to be issued a CAC in order to receive a WRNMMC badge, and he added that he was currently revising this instruction.

88. NSABETHINST 5530.2, 4(d)(1) "Access Control Procedures," dated 15 December 2011, states:

> All assigned WRNMMC personnel (military, government employees, contractors, vendors, or volunteers) regardless of purpose, must obtain and properly display the appropriate ID badge on the outer garment and conform to requirements and restrictions of this instruction, while within a designated WRNMMC building. ID badges will only be issued at the [NSAB] Pass and ID Office. All newly reported WRNMMC personnel are required to obtain an ID badge."

89. NSABETHINST 5530.2, paragraph 4d(4)(e), "Access Control Procedures," dated 15 December 2011, states:

> Contractors who are assigned to WRNMMC and also have a common access card (CAC) will be issued for a period not to exceed the length of their current or renewed contract, or one year, whichever is sooner. Contractors who are not eligible for CAC cards and vendors are no longer issued contractor WRNMMC ID badges and must register through RAPIDGate. Contractors will be identified by an ID badge with their name displayed in white letters on a blue stripe."

90. The CNIC Deputy Director of Operations (CNIC N3B) stated the wording in NSABETHINST 5530.2 caused confusion and seemed to

be ambiguous and disconnected. The CNIC N3B stated he interpreted the language in the instruction to mean that NSAB could issue a contractor employee, who possessed a CAC, a WRNMMC badge. He also read it to mean that if a contractor employee did not have a CAC, then he/she was not eligible to receive a WRNMMC badge.

91. The investigators consulted CNIC counsel and subordinate command legal offices regarding the confusion surrounding the wording in NSABETHINST 5530.2, 4d(4)(e). One of the three attorneys investigators consulted interpreted the paragraph to mean a contractor must have either a CAC or a RAPIDGate card to get a WRNMMC badge and that a contractor with a CAC did not require a RAPIDGate card to receive a WRNMMC badge. Two attorneys advised investigators that paragraph 4d(4)(e) was poorly written, difficult to interpret correctly, and failed to address the type of badge issued to contractors already issued a CAC card.

92. Subject 1 explained in an email message dated 11 August 2014 it was his understanding that in the December 2012 Government contractors would not be registered and/or included in RAPIDGate. Subject 1 stated that, in his mind, he defined Government contractors as "those contractors who report to work here (NSAB) daily and perform all of their work for NSAB." In support of his testimony, Subject 1 stated that CNICNOTE 5530, enclosure 1, paragraph 2(a), dated 26 April 2011, states:

> NCACS is designed to manage commercial vendors, contractors, sub-contractor, suppliers, and service providers (vendors/contractors) not authorized to receive a Department of Defense (DoD) Common Access Card (CAC), regardless of how they access the installation."[31]

93. Subject 1 further elaborated that CNICNOTE 5530 caused him to believe that RAPIDGate applied to commercial contractors, such as those who provided commercial services to the installation. Subject 1 stated that Kor Emp 1 was a Government contractor employee as opposed to a commercial contractor employee.

[31] Subject 1 stressed in his email message that RAPIDGate is a program that falls under the NCACS.

94. In addition to CNICNOTE 5530, Subject 1 also referenced CNICINST 5530.14, section 0410, dated 7 July 2011, which states:[32]

> Contractor personnel will not be issued a CAC until a need arises for an electronic card to gain physical access to controlled areas or logical access to Navy Marine Corps Internet [sic] (NMCI)."

Subject 1 further explained that WRNMMC employees were not necessarily required to gain access to NMCI. In addition, he stated that physical access to spaces in Building 27, where the ITD was located, was controlled by a different electronic system, over which NSAB and its Security Office had no control.

95. Subject 1 stated that after the disestablishment of NNMC, WRNMMC leadership announced that pending new issuance from WRNMMC all prior NNMC instructions would remain enforce. Subject 1 said he relied on NATNAVMEDCENINST 5527.1, which states:

> The results of the NCIC check will be the primary information used to approve or disapprove requests for NNMC access ID badges and/or access to work on the NNMC complex."

96. Subject 1 stated that he interpreted all of the above instructions to mean that contractors at WRNMMC were not required to be issued a CAC in order to gain access to the base.

97. Subject 1 testified that, NSABETHINST 5530.2, 4d(4)(e) did not include the requirement for a NCIC and, that in accordance with CNICINST 5530.14, he believed Kor Emp 1 was required to undergo an NCIC check. CNICINST 5530.14, CNIC Ashore Protection Program, section 0408, paragraph d(2)(e), 7 July 2011 states:[33]

> The establishment of standards for base access is ultimately the responsibility of the Installation Commanding Officer. Any adverse information identified during criminal history checks must be evaluated by a

[32] Subject 1 commented in his email message that CNICINST 5530.14 did not cancel CNICNOTE 5530, dated 26 April 2011.

[33] CNIC 5530.14 is a document entitled "Projected/Upcoming Changes to CNIC 5530.14" and the proposed changes within it were expected to be implemented by 30 April 2012.

competent individual designated by the Installation Commanding Officer, who is qualified in interpreting criminal record information. Likewise, positive mitigating factors should be considered into the final determination. The following minimum standards should be considered for denying installation access for a civilian employee, contractor/subcontractor, family members or non-affiliated civilians: 1) Any felony conviction within the past 10 Years, and 2) Any conviction of an offense meeting the sexual offender criteria in reference (y)."

98. CNICINST 5530.14 Enclosure 1, pg. H-10 Paragraph 4, Locally Issued Passes, provides:

a. Local SOP. Installations and Regions will establish individual SOPs to properly implement the guidance of Federal, DOD, Navy, and CNIC guidance. The SOPs will include detailed standards and procedures for the application, issuance, and the authentication of passes, including, at a minimum, the following:

(1) Processing. Must be processed at the Navy Visitor Control Center, under local and higher directive procedures.

(2) Vetting. Will undergo necessary personal identification and background checks including but not limited to:

a) National Criminal Investigation Check (NCIC) background check.

(b) Will meet the requirements as set forth in OPNAVINST 1752.3; Policy for Sex Offender Tracking, Assignment and Access Restrictions within the Navy.

99. OPNAVINST 1752.3 Paragraph 5 a. (2) provides:

a. Commander, Navy Installations Command (CNIC) shall:

. . .

(2) Establish procedure to identify sex offenders incident to application for housing assignment, base access, vehicle registration and renewal of identification cards.

100. Subject 1 stated that he first became aware there was an issue concerning Kor Emp 1 when he received an email from the Complainant on 9 September 2013 in stating Kor Emp 1 had not been properly vetted through the PSO, and therefore, should not have been granted a badge giving him access to the facility. According to Subject 1, the Complainant further requested that Kor Emp 1's access to WRNMMC be revoked immediately. Subject 1 testified that because the Complainant was not in his chain of command, and he did not have the authority to revoke an individual's access to the base, on 9 September 2013, he contacted the NSAB DSO, for guidance on how to respond to the Complainant's request.

101. On 11 September 2013, Subject 1 sent the Complainant an email informing him that he had forwarded the Complainant's request to revoke Kor Emp 1's badge and access to the base to the NSAB DSO and was awaiting his guidance. Subject 1 also stated that he informed the Complainant that debarring an individual from the installation required approval from the CO. The same day the Complainant replied to Subject 1 stating Kor Emp 1 should not have been granted a badge because he had not been approved for one. The Complainant further inquired as to what criteria the NSAB office used in granting Kor Emp 1 access to the base. Subject 1 stated that he instructed an employee in the NSAB Pass and ID Office, to pull Kor Emp 1's file. Subject 1 testified that he checked the file and determined Kor Emp 1 had a signed, approved memorandum form in his file.

102. On 17 September 2013, the NSAB DSO sent an email to the Complainant stating they had checked Kor Emp 1's record in NCIC and the Sex Offender Registry and found no record of criminal history; no record in the National Sex Offender public website; and no record in CLEOC. In the email, the Complainant was asked to identify the specific concerns he had regarding Kor Emp 1.

103. Subject 1 testified that the Complainant did not respond to the NSAB DSO' request that he provide further information regarding Kor Emp 1. Subject 1 also testified that the NSAB DSO informed him the NSAB ED made the decision to allow Kor Emp 1 to maintain his access to WRNMMC. Subject 1 further stated that the Complainant's request to revoke Kor Emp 1's access to the base concerned him as he had not been asked to do this for any other contractor or Government employee.

104. In an email message dated 7 August 2014, Subject 1 stated that he checked the NCIC log books on file and verified that no

one had conducted an NCIC check on Kor Emp 1 on or about 4 December 2012.

105. In his final interview, Subject 1 clarified his testimony about the NCIC checks by testifying he or his assistant conducted these checks on contractor employees who came to work at NSAB both before and after they started work in December 2012.

106. Despite their limited access to the needed resources, Subject 1 stated his office conducted NCIC checks on contractor employees in December 2012 if the Contracting Officer's Representative (COR) and/or the Contracting Officer's Technical Representative (COTR) sent the Pass and ID Office a base access request on an individual. The COR/COTR initiated the process they followed at that time; when Subject 1 and his assistant received the base access request form, they went to the NCIC terminal located in Dispatch and conducted the check. Subject 1 testified that he ran some of these NCIC checks on contractor employees himself in 2012 and estimated he conducted these checks perhaps 2 to 3 times a week. Sometimes the personnel in Dispatch would run the NCIC checks for him and his assistant at night and provide them with the results the next morning.

107. If they did not receive a request from the COR/COTR, Subject 1 said they did not conduct the NCIC check. Subject 1 testified that at the time they "trusted the COR/COTR would send them a request for base access for every contractor employee." In 2012, the NCIC check reviewed a person's criminal history, screened him or her as a registered sex offender, and also checked to determine if he or she was listed on a terrorist database. His office did not conduct CLEOC checks for debarment in 2012. Subject 1 did not recall his immediate supervisor instructing him to conduct NCIC checks at the time. Subject 1 testified that if the NCIC check developed derogatory information about a person, he and his assistant would discuss it with the NSAB DSO so that they could determine whether or not to grant the individual access to the installation.

108. Subject 1 testified he was not aware of any request for an NCIC check to be conducted on Kor Emp 1 in December 2012, and he stated he would not have remembered his name if such a request had been made at the time. There was nothing in place in December 2012 that would have enabled the Pass and ID Office to verify that an NCIC check had been done on Kor Emp 1 or other contractor employees like him on the MedPro/B.E.A.T. contract. Subject 1 confirmed that the first time he learned about any

issue related to Kor Emp 1's access to NSAB was in September 2013 when the Complainant emailed him about his concerns. Subject 1 testified that on 17 September 2013 he checked the NCIC log book for the terminal and noted that there was no record of an NCIC check having been conducted on Kor Emp 1 on or about 4 December 2012.

109. Regarding applicable instructions, Subject 1 stated in December 2012 he was aware that the installation, which was still the National Naval Medical Center, followed NATNAVMEDINST 5527.01. This instruction required that they run NCIC checks on contractor and government employees. Subject 1 explained the NCIC check was how they vetted the individuals prior to allowing them to access the installation. In addition to NATNAVMEDINST 5527.01, Subject 1 testified that he was also aware there were additional instructions in place in December 2012 that addressed base access and provided him with specific guidance on this issue. He cited both the NSABETHINST 5530.2 and the DTM 09-012 as being in place at the time, but said he did not remember if the CNICINST 5530.14, which was also in place then, required them to conduct NCIC checks.

110. Concerning the DTM 09-012, Subject 1 stated he reviewed the document in the past, and he recalled asking the NSAB DSO about the requirements contained within it. Subject 1 testified that he "sent the DTM 09-012 up his chain of command" to the NSAB DSO, the NSAB DSO's predecessor, a prior NSAB DSO, and the CO. He stated all these individuals instructed him to continue to follow the procedures they already had in place regarding the base access list. Subject 1 understood that he had been told to "stay the course" until such a time as new guidance on base access came from CNIC, the region, or the CO. When new guidance on this matter was issued, Subject 1 testified he made his chain of command aware of the documents and any relevant changes to base access procedures.

111. In December 2012, new employees brought in their documentation or the COR/COTR escorted them into the Pass and ID Office. The individual sponsor of military personnel who needed access to the base would escort them to the office.

112. Regarding visitors who requested access to NSAB in December 2012, Subject 1 testified that if the Pass and ID Office received an email request from someone on the base that an individual would be visiting, then his office would place the person's name on the base access list. They did not vet visitors in any way at the time, so if a visitor's name did not

appear on the base access list the person was denied access to NSAB. Subject 1 explained there were a variety of different forms of identification that a person could present in 2012 in order to be admitted onto the installation.

113. In the fall of 2013, Subject 1 testified they continued to check contractor employees in NCIC if they received a request to do so from the COR/COTR. Around that time Subject 1 explained that a new instruction also came out in May 2013, and he identified that as CNICINST 5530.14A. Subject 1 explained that CNICINST 5530.14A was important in that it required the Pass and ID Office to run NCIC checks on new employees, such as contractors, and visitors who requested access to NSAB. The NCIC check looked at an individual's criminal history, such as any felony convictions, screened to see if they were a registered sex offender, and checked to determine if they were considered to have any terrorist connections. Subject 1 told us he discussed this new instruction with the NSAB DSO when it was issued, and shortly after that the Pass and ID Office began to receive additional NCIC terminals. Around this time, the former CO, NSAB instructed him to continue to provide a base access list to the staff at the front gate to NSAB. Approximately in September 2013, the current CO, informed Subject 1 that they would begin to follow CNICINST 5530.14A. As a result of this, Subject 1 stated that his office began to conduct NCIC checks.

114. By 30 September 2013, Subject 1 testified that additional NCIC terminal were installed on the base and this improved the Pass and ID Office's ability to conduct the NCIC checks on government contractor employees.

**Regulations**

115. Section 1069, Standards Required for Entry to Military Installations in United States, of the FY 2008 NDAA states, in pertinent part:

> (a) DEVELOPMENT OF STANDARDS.—
>
> (1) ACCESS STANDARDS FOR VISITORS.—The Secretary of Defense shall develop access standards applicable to all military installations in the United States. The standards shall require screening standards appropriate to the type of installation involved, the security level, category of individuals authorized to visit the installation, and level of access to be granted, including—

(A) protocols to determine the fitness of the individual

(B) standards and methods for verifying the identity of the individual.

(2) ADDITIONAL CRITERIA.—The standards required under paragraph (1) may —

(A) provide for expedited access to a military installation for Department of Defense personnel and employees and family members of personnel who reside on the installation;

(B) provide for closer scrutiny of categories of individuals determined by the Secretary of Defense to pose a higher potential security risk; and

(C) in the case of an installation that the Secretary determines contains particularly sensitive facilities, provide additional screening requirements, as well as physical and other security measures for the installation.

116. DTM 09-012, Interim Policy Guidance for Physical Access Control, Change 2 of 9 September 2012[34], Attachment 3, Physical Security Access Control Standards, states in paragraph 2:

PROOFING AND VETTING. The access control standards shall include identity proofing; determining the fitness of an individual requesting and/or requiring access to DoD facilities; and vetting.

b. Non-Federal Government and non-DoD-issued card holders who are provided unescorted access require identity proofing and vetting to determine fitness and eligibility for access.

(1) Persons requesting access shall provide justification and/or purpose for access to DoD facilities.

(2) Persons requesting access that are not in possession of an approved, Government issued card shall provide a document listed in Attachment 4. The documents

[34] Initially issued December 8, 2009. Changes 1 through 4 have been issued only to extend its expiration date.

presented shall be reviewed by an authorized Government representative for the purposes of identity proofing.

(3) The local commander and/or director shall determine the recurring requirement and frequency for additional checks of non-Federal Government and non-DoD-issued card holders based upon local security requirements using Government authoritative databases only as prescribed herein.

(4) Installation government representatives shall query the following government authoritative data sources to vet the claimed identity and to determine fitness, using biographical information including, but not limited to, the person’s name date of birth, and social security number:

(a) The National Crime Information Center (NCIC) database.

(b) The Terrorist Screening Database.

(c) Other sources as determined by the DoD Component or the local commander and/or director. These can include but are not limited to:

1. Department of Homeland Security (E-Verify).

2. Department of Homeland Security (U.S. VISIT). DTM 09-012, December 8, 2009

3. Department of State Consular Checks (non-U.S. citizen).

4. The FVS-CM.

(5) Only personnel delegated by the installation commander shall perform access control duties that include:

(a) Identity proofing.

(b) Vetting and determination of fitness.

(c) Access authorizations and privileges.

(6) Installation personnel will issue the appropriate card and/or pass, as authorized.”

117. In July 2011, CNIC issued CNIC Instruction (CNICINST) 5530.14, CNIC Ashore Protection Program, July 7, 2011. Enclosure (1), section 0403, of CNICINST 5530.14 states CNIC's policy to "implement policy guidance [in accordance with DTM 09-012] to establish minimum security standards for controlling entry to Navy installations."

118. CNICINST 5530.14 recognized four means by which contractor employees may access Navy installations: by presenting a CAC based upon a NACI check for contractor employees requiring logical access to DoD information systems; a Transportation Workers Identification Card (TWIC) issued by the Department of Transportation; a Navy Commercial Access Control System (NCACS) card based upon a commercial background check reasonably equivalent to that required by DTM 09-012; or a visitors pass or local credential issued according to local installation procedures.

119. CNICINST 5530.14 also incorporated information in earlier issuances establishing the NCACS, also known as RAPIDGate. NCACS is a voluntary system that allows commercial contractors to purchase identity proofing and vetting services from an approved Navy contractor so that their individually vetted employees may enter Navy installations repeatedly without having to undergo identity proofing and vetting each time they access a Navy installation. NCACS was designed by Navy to manage recurring vendors, contractors, suppliers and other service providers who are not authorized a CAC. CNIC characterizes NCACS as an economical and efficient method to identity proof and vet commercial contractors doing business routinely aboard Navy installations.

120. CNIC policy guidance provides, in CNICINST 5530.14, Enclosure (1), Section 403, paragraph a., that access control standards shall include:

> (1) Identity validations
>
> (2) Determining the suitability of an individual requesting and/or requiring access
>
> (3) Vetting

121. The instruction, however, did not direct Navy installation personnel to conduct NCIC and Terrorism Screening Database checks on non-Federal and non-DoD card holders prior to authorizing them unescorted access to a Navy installation. Instead, it required installation commanding officers to

implement SOPs that would require the checks. CNICINST 5530.14, section 409.d., establishes NCACS installation responsibilities as follows:

> (2) Each Installation will establish a NCACS SOP and Post Orders using Appendix H, CNIC NCACS SOP as a template.
>
> (3) Installations will maintain a 1-day Visitor Pass program for those non-CAC vendors/contractors who choose not to enroll in the NCACS.
>
> (a) Installations will ensure, as per local implementing SOPs, that Visitor Passes are issued in compliance with Federal, DoD, DON and CNIC guidance.

122. The Sample NCACS SOP included in CNICINST 5530.14 at Enclosure 1, Appendix H, which applies to contractors and contractor employees who are not issued a CAC, provides on page H-10, Paragraph 4, Locally Issued Passes:

> a. Local SOP. Installations and Regions will establish individual SOPs to properly implement the guidance of Federal, DOD, Navy, and CNIC guidance. The SOPs will include detailed standards and procedures for the application, issuance, and the authentication of passes, including, at a minimum, the following:
>
> (1) Processing. Must be processed at the Navy Visitor control Center, under local and higher directive procedures.
>
> (2) Vetting. Will undergo necessary personal identification and background checks including but not limited to:
>
> (a) National Criminal Investigation Check (NCIC) background check.
>
> (b) Will meet the requirements as set forth in OPNAVINST 1752.3; Policy for Sex Offender Tracking, Assignment and Access Restrictions within the Navy.

123. OPNAVINST 1752.3 Paragraph 5 a. (2) provides:

> a. Commander, Navy Installations Command (CNIC) shall:
>
> (2) Establish procedure to identify sex offenders incident to application for housing assignment, base

> access, vehicle registration and renewal of identification cards.

124. Under the provisions of CNICINST 5530.14, section d(3)(g), unescorted visitors requesting a short term installation visitors pass required only an installation sponsor request, valid federal or state identification, e.g., driver's license, and vehicle registration and insurance if driving a motor vehicle, a Sex Offender Registration and Notification Act of 2006 (SORNA) check and a debarment check using the Consolidated Law Enforcement Operations Center (CLEOC) database. Contractors and contractor employees who are not issued a CAC and who choose not to participate in NCACS may access the installation under the local installation visitor access procedures.

125. The CNIC instruction also required each installation to issue an NCACS Standard Operating Procedure (SOP) using the template provided in Appendix H to the instruction. That template includes provisions requiring contractors who do not participate in NCACS to undergo the criminal checks specified by DTM 09-012, and specifically identifies the NCIC index and Terrorist Screening Database checks as those that will be performed. If an installation failed to issue the SOP, however, there is no express language in the CNIC instruction itself that required the DTM 09-012 specified NCIC and Terrorism Database checks be performed by installation access personnel prior to authorizing entry of contractor employees or other installation visitors. While the CNIC instruction may not have imposed a direct responsibility on installation access personnel to conduct required NCIC and Terrorism Database checks, the higher level guidance upon which the CNIC instruction's vetting and identity proofing requirements were based, DTM 09-012, imposed such requirements on NSA Bethesda installation access personnel.

126. Although issued after CNICINST 5530.14, NSABETHINST 5530.2, Access Control Procedures, December 15, 2011, which was in effect during the period relevant to this investigation, did not refer to the CNICINST. Instead, the NSA Bethesda instruction referenced the authority of DTM 09-012 and of OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program, January 28, 2009, which was issued prior to the DTM.

127. OPNAVINST 5530.14E requires that, "[Installation Commanding Officers] shall publish a process for removal of, or denying access to, persons who are not authorized or represent a criminal threat." It does not establish specific vetting requirements for entry onto Navy installations.

128. Even though NSABETHINST 5530.2 referenced the DTM, however, it did not implement the standards specified in the DTM for vetting visitors by conducting NCIC and Terrorism Database checks. Instead the NSAB instruction appeared to require only verification of identity and purpose for entry for most visitors. The instruction did not require vetting based on a criminal history check prior to allowing unescorted entry for non-Federal and non-DoD issued card holders.

129. NSABINST 5530.2 authorized persons issued a WRNMMC badge to access the NSAB installation. The following provisions applied to issuance of WRNMMC badges for contractor employees:

> d. Issuing of Walter Reed National Military Medical Center Bethesda (WRNMMCB) Identification (ID) badges.
>
> (1) All assigned WRNMMC personnel (military, government employees, contractors, vendors, or volunteers) regardless of purpose, must obtain and properly display the appropriate ID badge on the outer garment and conform to requirements and restrictions of this instruction, while within a designated WRNMMC building. ID badges will only be issued at the NSA Bethesda Pass and ID office. All newly reported WRNMMC personnel are required to obtain an ID badge.
>
> .....
>
> (4) WRNMMC badge guidelines and color-codes.
>
> (e) Contractors. Contractors who are assigned to WRNMMC and also have a common access card (CAC) will be issued for a period not to exceed the length of their current or renewed contract, or one year, whichever is sooner. Contractors who are not eligible for CAC cards and vendors are no longer issued contractor WRNMMC ID badges and must register through RAPIDGate. Contractors will be identified by an ID badge with their name displayed in white letters on a blue stripe."

130. NATNAVMEDCENINST 5527.1 provides in pertinent part as follows:

> 4. Policy.
>
> (a) Per reference (a)[DoDINST 2000.16, DoD Antiterrorism (AT) Standards, October 2, 2006] all contractual employees will be subject to a trustworthy

determination check by the NNMC Security Department through the National Crime Information Center (NCIC). This check will be completed and approved prior to issuance of an NNMC access identification badge, or access to NNMC complex is continued to be authorized for contractual personnel who are not issued an NNMC access ID badge.

b. Approval or disapproval for access and/or issuance of an NNMC access ID badge will be based on criteria outlined in current NNMC Security Standard Operating Procedures (SOP).

5. Action.

.....

c. The results of the NCIC check will be the primary information used to approve or disapprove requests for NNMC access ID badges and/or access to work on the NNMC complex."

**Discussion and Analysis**

131. Section 1069 FY2008 NDAA requires SECDEF to develop screening standards pertaining to access of military installations in the United States. In December 2009, the Under Secretary of Defense for Intelligence (USD(I)) issued DTM 09-012, “Interim Policy Guidance for DoD Physical Access Control,” to implement the standards mandated by section 1069, NDAA 2008. DTM 09-012 established the minimum DoD standards for determining fitness and verifying the identities of all persons requesting access to DoD installations and directed DoD components, including DON, to implement the standards no later than October 1, 2010, "as resources, law, and capabilities permit."[35]

132. Under the minimum standards for access established by DTM 09-012, all persons requesting unescorted access to a DoD installation require identity proofing and vetting to determine their fitness and eligibility for access. Visitors not eligible for CAC, PIV, TWIC or DoD Identification cards must be screened by an authorized government representative upon entry to determine that they have a valid reason to enter the base, to verify their identity and to ensure that their character or conduct does not threaten the security of the installation, its resources or personnel. The DTM requires visitors, including

[35] DTM 09-032 has been reissued regularly since 2009 pending its incorporation into permanent DoD regulations.

most contractors, to present an approved identification document and submit to law enforcement background checks prior to entry. Required law enforcement checks include:

a. National Crime Information Center (NCIC) Database;

b. the Terrorist Screening Database; and,

c. other sources as determined by the DoD component or the local commander and/or director.

133. In accordance with DTM Attachment 3, paragraph 2b(4)(c), the OPNAVINST 1752.3 and CNICINST 5530.14 included provisions requiring Sex Offender Registry checks. CNICINST 5530.14 also mandated local no entry and installation debarment checks be conducted prior to allowing an individual access to the installation.

134. Subject 1's PD, as the ACO, assigned him responsibility for the overall management of the NSAB installation access control program, issuance of WRNMMC hospital identification cards, registration of privately owned vehicles, and the qualification and authorization for personnel to enter the installation. In this capacity, as stated in his PD and in CNICINST 5530.14, Subject 1 was required to be thoroughly familiar and highly knowledgeable of DoD and DoN physical security instructions, policies, and related guidance necessary to establish compliance with DoN requirements.

135. We conducted three separate interviews with Subject 1 in order to reconcile the various discrepancies in his testimony concerning his understanding of the applicable regulations, his knowledge of the access control process for contractor employees, and the specific circumstances regarding Kor Emp 1 receiving access to the installation. After considering all his testimony and subsequent follow up emails, we ultimately determined that as early as December 2012 Subject 1 was aware that NSAB's Pass and ID Office had a responsibility to conduct NCIC checks on contractor employees seeking access to the NSAB installation prior to issuing them a WRNMMC badge.

136. Regarding the applicable regulations, we noted there was considerable confusion about the requirements; however, we determined Subject 1 was aware of both DTM 09-012 and CNICINST 5530.14, but he also testified that he understood NSAB adhered to NATNAVMEDCENINST 5527.1 and NSABETHINST 5530.2 with respect to the base access requirements in December 2012. We determined that although NSABETHINST 5530.2 did not provide provisions for

conducting an NCIC check, the higher authority instructions, DTM 09-012, CNICINST 5530.14 and NATNAVMEDCENINST 5527.1, clearly specified an NCIC check was required prior to allowing access to the installation or the issuance of a WRNMMC badge. DTM 09-012 further required a screening of the Terrorist Database and CNICINST 5530.14 required a Sex Offender Registry check also be conducted.

137. Concerning NSAB's access control processes, we determined that in December 2012 Subject 1, as the ACO, was aware he was responsible for ensuring that NCIC checks were conducted for contractor employees reporting for work aboard the installation. He acknowledged the NCIC checks did not always occur due to both limited resources and confusing instructions. We determined that the NSAB access control procedures also relied heavily upon the COR/COTR sending them a request for base access for an individual in advance of the person reporting for work at NSAB, and it was this request that initiated the entire process. If the COR/COTR submitted a request, Subject 1 or his assistant conducted the NCIC check on an individual; conversely, if the COR/COTR failed to submit a base access request form for a contractor employee, then Subject 1, as the ACO, and his staff would not have been aware that an NCIC check was needed.

138. In the case of Kor Emp 1, we determined there was no record in the NSAB NCIC log books that he underwent an NCIC check on or about 4 December 2012, and Subject 1 testified that he did not conduct an NCIC check on him until the NSAB DSO requested he do so on 17 September 2013. Although the September 2013 NCIC check on Kor Emp 1 did not develop any derogatory information on him, we concluded, nonetheless, that Subject 1 failed in his duty as the ACO to conduct the NCIC check on Kor Emp 1 before granting him access to NSAB and issuing him a WRNMMC badge in December 2012.

**Conclusion**

139. The allegation is **substantiated**.

**Recommendations**

140. That NSAB revise NSABETHINST 5530.2 to incorporate the requirements set forth in CNICINST 5530.14A and DTM 09-012. Specifically, the installation access control standards should include requirements for conducting NCIC index, Sex Offender Registry, Terrorist Screening Database, and debarment checks to

determine the fitness of an individual requesting and/or requiring access credentials.

141. As currently written, the NSABETHINST 5530.2 4d(4)(e) allows conflicting interpretations with regards to issuing WRNMMC badges to contractors. Recommend NSAB clarify the requirement in this paragraph.

142. That CNIC ensure that lessons learned from this event are widely distributed with action directed to all Navy Regions Commanders to review procedures at all subordinate Naval Support Activities under their command.

**Actions Planned or Taken**

143. In October 2013, NSAB acquired six NCIC terminals, five of which are located in the NSAB Pass and ID Office. Given this added capability, personnel working in the Pass and ID office are able to conduct all NCIC checks from their work center.

144. On 14 August 2014, NSAB's new Pass and ID SOP went into effect. In accordance with this SOP, all in-processing employees and contractors are required to undergo NCIC, Sex Offender Registry, and debarment checks.

145. A memo released by the NSAB ED, Subject: NEW BASE ACCESS PROCEDURES FOR NSA BETHESDA named Subject 1 as the point of contact. The memo stated that effective 1 October 2014, the WRNMMC, USUHS and AFFRI ID badges will no longer be accepted for access through NSAB Entry Control Points (ECPs). All persons not on an approved access list and desiring to access NSAB will do so utilizing an approved credential (CAC, Uniform Service ID, NSAB ID/Temporary Pass, NCACS, Civil Service Retiree ID, VA ID) or they will be escorted by a Trusted Agent.

146. During the week of 25 August 2014, DoD IG conducted an audit of the NSAB Pass and ID office. This was a follow-up to the audit DoDIG-2013-134 (Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks) that was issued on 16 September 2013. The IG DoD review was ongoing at the time we concluded our investigation and a final report will not be published until February 2015.

**Personnel Actions Taken**

147. Subject 1 and his leadership all candidly spoke about the confusing language in NSABETHINST 5530.2 concerning what a contractor employee had to have in order to be issued a WRNMMC

badge to access NSAB. Even before the investigation into this allegation started, Subject 1 had already been assigned to work on a revision to this instruction as early as March 2013. The revised instruction will clarify the section that addressed contractors in order to eliminate future confusion, difficulties, or the potential for future allegations of violations. According to Subject 1 and his supervisors, the revision is underway. With that said, Subject 1 was required to follow the policy set forth in the CNICINST which required a higher-level of scrutiny than the local NSABETHINST to determine whether to allow a contractor employee on a base.

**Allegation Two**

> That, between September 2012 and November 2013, NSAB failed to follow identity proofing and vetting requirements prior to allowing IT Department contractors access to NSAB, in violation of Section 1069 of the FY2008 NDAA and its implementing regulations.

**Findings of Fact**

148. WRNMMC contracted with MedPro, LLC,[36] to provide IT Helpdesk services from 28 September 2012 through 19 November 2013. Within the MedPro, LLC, Contract W91YTZ-12-C-0157 15.11, the General Security Requirements states:

> Contract personnel or any representative of the contractor entering WRNMMC shall abide by all security regulations, acquiring and maintaining all necessary clearances. Subject to security regulations, the Government will provide the contractor access to the Installation to perform the tasks required under this contract. Contractor personnel may encounter data covered by the Privacy Act of 1974, and shall protect such information in accordance with AR 380-5. Contractor personnel must obtain and wear an identification badge provided by WRNMMC at all times while present in the facility. Each employee shall complete any and all security courses that are provided and mandated by the Government prior to employment consistent with Army, and DoD mandates. Contractor personnel and property shall be subject to search and seizure upon entering or leaving the confines of WRNMMC."

[36] MedPro, LLC, subcontracted with B.E.A.T.; this report refers to their combined services as MedPro/B.E.A.T. contract.

149. As already discussed in Allegation One, Subject 1 testified that the NSAB Pass and ID office issued WRNMMC badges to other MedPro/B.E.A.T. contractors besides Kor Emp 1, giving them access to NSAB and the WRNMMC facilities during the period in question.

150. On 20 August 2014, MedPro/B.E.A.T. provided investigators with the names of the 36 WRNMMC Helpdesk support contractor employees who provided the contractor services on the contract from 28 September 2012 to 19 November 2013. Subject 1, acknowledged that NCIC and Sex Offender Registry checks were not conducted for any of these 36 contractor employees during this timeframe. Explaining the oversight, Subject 1 stated in an e-mail to investigators on 21 August 2014:

> I just returned from spending a few hours in [the NSAB] Pass and ID searching the NCIC logs. None of the contractors had an NCIC check unless they checked in after our new Pass & ID SOP went into effect on 14 AUG 2014. After that, all in-processing employees and contractors are required to undergo an NCIC, sex offender, and debarment check. Prior to that, but after implementing NCIC in Pass and ID on approximately 30 SEP 2013 only visitors who picked up a pass, volunteers, constructions workers, vendors without a DoD ID, MWR employees, and RAPIDGate customers received these checks, as well as any suspects encountered on the patrol side of Base Police.

151. We noted that of the 36 contractor employees referenced in Subject 1's e-mail, NSAB records show that only 22 individuals were issued a WRNMMC badge. We were unable to locate any information regarding the remaining 14 employees.

152. As previously discussed in Allegation One, we determined that the current and former CO, NSAB, failed to ensure that NCIC index and Sex Offender Registry checks were conducted prior to the issuance of an installation access badge to these contractor employees. We determined that the former CO, NSAB was aware of the "vetting" process requirement for individuals requesting access to the installation before being granted a badge or access to the base. In his testimony, the former CO, NSAB stated, "somewhere we were on the hook for vetting… I don't want criminals and sex offenders accessing my base, right?" However, when we inquired into what the requirements were for obtaining a WRNMMC badge, he stated, "Did we then do any sort of additional, you know, background check on them before we issued them one [WRNMMC badge]? And my answer is I don't know what our exact

process was at the time." He further stated that he relied on Subject 1 and his office to handle processing contractor employees and issuing them the appropriate ID to access NSAB. In his response to the Complainant's 23 September 2013 letter to SECDEF, the current CO, NSAB sent an Info Memo to the Commandant, NDW, stating, "Per reference (d) [CNICINST 5530.14A], NSAB's access control procedures contain identity proofing and vetting measures to determine the fitness of an individual requesting and/or requiring access prior to the issuance of a local access credential or pass… The individual is subjected to criminal history and Sex Offender Registration and Notification Act (SORNA) checks through the Maryland Electronic Telecommunications Enforcement Resource System/National Crime Information Center (METERS/NCIC) and through the Navy's Consolidated Law Enforcement Operations Center (CLEOC) to determine fitness of the individual and ensure they are not currently barred from a Navy installation." However, as cited above, we determined that at least 22 of the 36 contract employees working during the period under review received a WRNMMC badge without having first undergone an NCIC or Sex Offender Registry check.

**Regulations**

153. The regulations discussed in the regulations section of Allegation One apply to this allegation.

**Discussion and Analysis**

154. In the case of these approximately 20 additional contractor employees who accessed NSAB in order to perform their duties under the MedPro/B.E.A.T. contract, we determined the same set of facts discussed in Allegation One applied. Subject 1 testified that he was aware that the applicable regulations required that he or his staff perform a NCIC and Sex Offender Registry checks on these individuals before providing them with WRNMMC badges and access to the installation. He admitted that they failed to perform these required security checks. He also acknowledged they failed to conduct these checks throughout the period of the contract even though the facility had additional NCIC terminals as early as October 2013 and could have performed those checks at the time.

155. As we previously stated in the discussion for Allegation One above, testimony obtained during the investigation from several managers within Subject 1's chain of command showed that they were not sufficiently engaged in the NSAB base access

control and WRNMMC badge issue processes as it pertained to the MedPro/B.E.A.T. contractor employees. For example, we noted that Subject 1's immediate supervisor, Deputy Security Director, NSAB, acknowledged in his interview that he allowed Subject 1 to "run the access process" at NSAB, and gave the impression that he (the supervisor) was not involved in the day-to-day operations of the NSAB Pass and ID Office. Although the NSAB DSO, Subject 1's second level supervisor, was not working in Security at NSAB when Kor Emp 1 was issued a badge in December 2012, the NSAB DSO testified that he assumed his current duties starting in March 2013. He was present, therefore, during the remaining period of the MedPro/B.E.A.T contract and at a time when some of the other IT contractor employees worked at WRNMMC. The NSAB DSO also testified that NSAB had not documented the process of issuing WRNMMC badges in writing; he acknowledged, however, that Subject 1 had been tasked to revise the NSABETHINST 5530.2 as early as March 2013, but the revised instruction was not completed by the time of our interviews. From March 2013 to the present the NSAB DSO had a responsibility to conduct appropriate oversight of Subject 1 and his Pass and ID Office staff, but his testimony indicated that he was not as engaged as he could have been in overseeing the process. Finally, the testimony of the NSAB ED indicated a lack of managerial involvement when he admitted to the investigators that he was aware NSAB was not following its own instruction on issuing badges properly; the policy was not yet in a written format; and they followed more of a "word of mouth" policy with the medical center. He further stated NSAB would begin to adhere to a written policy effective 1 October 2014.

156. Also as previously discussed in Allegation One, we further determined that the current and former CO, NSAB, did not ensure that base access controls were properly directed; the NSABETHINST 5530.2 they were responsible for issuing was not sufficiently clear and likely contributed to the skipped background checks. The foregoing management oversight failures notwithstanding, we concluded that Subject 1 understood the requirement to submit the MedPro/B.E.A.T. contractor employees for the required background checks before allowing them access to NSAB or issuing them a WRNMMC badge, but he failed to do so.

**Conclusion**

157. The allegation is **substantiated**.

**Recommendations**

158. That NSABETHINST 5530.2 be rewritten to incorporate the requirements set forth in CNICINST 5530.14A. Specifically, the installation access control standards should include requirements for conducting NCIC, Sex Offender Registry, and debarment checks to determine the fitness of an individual requesting and/or requiring unescorted access credentials. As currently written, the instruction allows conflicting interpretations with regards to the issuing of contractor badges.

159. That CNIC direct all Navy Regions to screen all current contractor employees to ensure that they were submitted for a NCIC, Sex Offender Registry, and debarment check before they were issued their current installation access credential and anyone found to have not undergone these checks be immediately submitted for such checks. Anyone found not in compliance with access requirements set forth in CNICINST 5530.14 shall thereafter have their installation access revoked.

160. That CNIC ensure that lessons learned from this event are widely distributed with action directed to all Navy Region Commanders to review procedures at all Naval Support Activities under their command.

**Actions Planned or Taken**

161. In October 2013, NSAB acquired six NCIC terminals, five of which are located in the NSAB Pass and ID Office. Given this added capability, personnel working in the Pass and ID office are able to conduct all required NCIC checks from their work center.

162. On 14 August 2014, NSAB's new Pass and ID SOP went into effect. In accordance with this SOP, all in-processing government and contractor employees are now required to undergo NCIC, sex offender, and debarment checks.

163. IG DoD audit personnel visited the NSAB Pass and ID office the week of 25 August 2014 to perform a follow-up of Recommendations A.1 and A.3 from their audit mentioned earlier in this report. [37] However, the auditors have not completed

[37] DoDIG-2013-134, Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks, 16 September 2013

their analysis of NSAB and anticipate that a final report will be published around the beginning of CY 2015.

164. WRNMMC and NSAB will continue to provide a security system that ensures security checks of all personnel entering NSAB while maintaining safe, prompt, and efficient access for patients and their family members. NSAB and WRNMMC will coordinate their procedures to ensure they do not impede patient access to care and priority access to military and family members.

**Allegation Three**

Allegation Three: That, between September 2012 and November 2013, WRNMMC allowed IT Department contractor employees access to Government IT systems without first obtaining the results of a National Agency Check with Inquiries (NACI), in violation of the DoD policy established in 5200.2-R, DoD Personnel Security Program.

**Findings of Fact**

165. The Complainant alleged approximately 20 contractors gained access to Government IT systems, which may contain PII, sensitive information, and/or classified information prior to having a BI/SC completed. The Complainant identified Kor Emp 1 as one of the contractor employees, but did not provide the names of the others.

166. The WRNMMC Chief Information Officer (CIO) and ITD Chief testified that WRNMMC IT contractor employees did not work with classified information. Moreover, the WRNMMC ITD Chief explained that the WRNMMC ITD did not handle classified information at all; he testified: "We don't have classified material here at all."

167. During his assignment to WRNMMC, the former Deputy Commander for Administration (DCO-Admin)[38] was responsible for overall operation of the following departments:

(1) Information Management and ITD consisting of one officer (the WRNMMC ITD Chief), 168 contractors, 28 Government civilians, and 16 enlisted members

The WRNMMC ITD Chief, Chief Information Officer (CIO)

[38] This individual retired on 1 October 2013.

Deputy CIO; Contracting Officer Representative (COR) (DWNMMC CIO/COR) on the MedPro/B.E.A.T. contract and other contracts; Subject 1 Chief Operations Officer (COO); Chief of Support Services, Chief of Server & Data Center, Chief of Telecom, Chief of Network Operations One-Stop Help Desk

Chief Technology Officer

Chief Information Management Officer

Information Assurance Officer

(2) Human Resources and Manpower consisting of 2 officers (Subject 2 and his Assistant Department Chief), 22 Government civilians, 14 enlisted members, and 7 contractors

Subject 2, Chief, HR and Manpower

Complainant Personnel Security

Manpower and Documentation

Civilian Personnel

Military Personnel

Defense Military Health Resources System-internet (DMHRSi)[39]

(3) Facilities;

(4) Logistics;

(5) Nutrition Services; and,

(6) Patient Administration

168. According to Subject 1, newly-reporting contractor employees used a Check-In sheet to complete in-processing into the command. The contractor employees' last four SSN#, title of their position, and ITD, were listed at the top on the form. Listed also in a table on the form were the departments/offices the contractors were required to have initial or stamp to

[39] The Defense Medical Human Resource System - internet is a web-based Tri-Service decision support system that enables the MHS to manage medical human resources across the enterprise by allowing ready access to essential manpower, personnel, labor cost assignment (MEPRS), education and training and personnel readiness information.

complete the Check-In process. The sample form below shows the majority of offices to which the contractor reported at WRNMMC and NSAB:

| Information Technology Department<br>Contractor Check-In Sheet<br>WRNMMC In-Processing | | |
|---|---|---|
| Stamp (Initials) | Department | Purpose |
| | ITD Administration/ Information Assurance | Pickup Welcome Package, Complete forms, Add to Roster & Recall |
| | Security Office, Complainant's PSO Coworker (Civ); [Complainant] (Con)[40] | Sign SAAR form; initiate background/clearance |
| | DMHRSi | Register for DMHRSi access |
| | ITD One Stop Shop | Establish computer accounts |
| | Personnel Support Detachment (PSD) | Common Access Card Issuance (must have 2 forms of ID) |
| | Pass and ID Security[41] | Obtain Staff Badge, Register Vehicles, Parking Pass |
| | DMHRSi | Drop off ALL remaining forms and check-in sheet |

169. As noted in the table above, the Complainant was responsible for processing the contractor employees' SAAR form. The SAAR-N is a four-part form used to authorize anyone requiring access to the WRNMMC IT network. Part I is filled out by the requestor (e.g., contractor employee) requesting access and Part II is endorsed by the government employee (ITD Chief) assigned responsibility for oversight of the contractor employee's work. The endorsement in Part II did not grant the requestor access to the IT system; it was simply an appropriate government official's acknowledgement that the requestor had a

[40] Con - contractors

[41] The Pass and ID Security Office, where Subject 1 worked, was the NSAB Visitor's Center, Building 102. DMHRSi, PSD, and the Security Office, where the Complainant worked, were all in Building 17A. ITD Administration was in Building 27.

legitimate requirement for access to the IT system to perform their official duties. Part III required the WRNMMC PSO CSM (Complainant's PSO Coworker until June 2013 when Subject 2 relieved Complainant's PSO Coworker as the CSM and assigned the Complainant as the Acting CSM) to validate the requestor's BI or SC information. Once the CSM completed the BI and SC check, the requestor submitted the form to the IT staff member (technician) responsible for setting up the requestor's IT network account. The IT staff member would then complete Part IV, noting the kind of access (system, domain, server application, data sets, etc.) granted.

170. We note here that the Personnel Security Office, Human Resource Office, Deputy Commander for Administration, Prospective Employee Profile Sheet was a separate form generated by Subject 2's department to in-process prospective employees. This form was used in conjunction with the ITD In-Processing Check-In Sheet, and in addition to the SAAR-N form described above.

171. The contractor employee MedPro assigned as the Program Manager, in this case Kor Emp 1, requested the contractor employee fill-in the requested information to include the full name, SSN#, date of birth, phone number, e-mail address, work space, and performance period. The PM then hand-carried all three forms, the ITD In-Processing Form, Prospective Employee Profile Sheet, and the SAAR-N Form while escorting the contractor employees to the various offices listed on the ITD Check-In Sheet.[42] When the PM and the contractor employee went to the PSO, the person assigned to conduct the background check on the contractor employee, in this case the Complainant, filled in the portion of the Prospective Employee Profile Sheet section entitled "FOR PERSONNEL SECURITY OFFICE PERSONNEL ONLY":

> Type of Investigation
> Opened Date; Closed Date
> Eligibility Date
> CAF Determined Eligibility of:
> Approved to In-Process Date
> Disapproved to In-Process Date
> PSO Official Signature

172. The PSO (Security Office) signed Part III of the SAAR-N form and initialed or stamped the ITD In-Processing Check-In Sheet to document the BI/SC information. The PM would then

[42] This is why Kor Emp 1 had access to the PII of Kor Emp 2, his co-worker.

escort the contractor employee to the One Stop Shop to request one of the technicians create a WRNMMC computer account.

173. Subject 2 stated the Complainant was responsible for the Check-In process at the PSO and that the contractor employees would report to the Complainant to have him conduct the necessary check in JPAS for the BI/SC information. Subject 2 testified that all WRNMMC personnel, including contractors, go through the same process of checking into the command. He said he believed the contractor employees were required to check-in with the PSO before the ITD provided access to the network. Subject 2 stated the Employee Profile Sheet never came to him for signature and that the PSO had responsibility for this process.

174. On 28 September 2012, U.S. Army Medical Command, Health Care Acquisition Activity, Northern Atlantic Region Contracting Office (NARCO), Fort Belvoir, Virginia, issued contract W91YTZ-12-C-0157 to MedPro Technologies, LLC, with B.E.A.T. as a subcontractor. The period of performance was 28 September 2012 thru 19 November 2013, as extended, and the contract required 20 Full-Time Equivalent (FTE) positions. Paragraph 2.1 of the contract states:

> WRNMMC requires on-site Clinical IT Customer Support Service Desk support. The contractor shall provide adequate services for WRNMMC to facilitate the successful accomplishment of the IT help desk mission.

175. MedPro, LLC, contract W91YTZ-12-C-0157, section 15.7, states:

> All DoD contractors whose duties are in the Information Technology and Telecommunications (ITT) and Information Assurance (IA) areas will be assigned a position sensitivity of IT-I or IT-II. Personnel designated as an IT-1 must obtain and maintain a Single Scope Background Investigation (SSBI). Personnel designated as an IT-II must obtain and maintain a National Agency Check with Local Agency and Credit Check (NACLC). WRNMMC FSO [Facility Security Officer] will forward the requests for background investigations to the Office of Personnel Management within 3 working days of receipt of all required paperwork.

176. MedPro, LLC, contract W91YTZ-12-C-0157, Section 5.1.4.1 states:

> All positions are ADP/IT-II: Non-critical-Sensitive. The required investigation is a National Agency Check with Law Enforcement and Credit (NACLC).

177. A CNIC Security Specialist explained that the NACLC is a higher level of background check than the NACI.

178. The MedPro LLC General Manager testified that the contract with WRNMMC did not require any security clearance level; it only required that employees have a NACLC.

179. The OSC letter referred to TASKORD R101210.01, Subject: BRAC TRANSITION NAVY IT ACCESS, stating “IT Level I designates a critical sensitive position in which there is a "potential for grave to exceptionally grave impact and/or damage," and an IT Level II designates a non-critical position, which has a "potential for some to serious impact and/or damage."

180. TASKORD R101210.01,[43] paragraph 3a(1), dated 7 December 2010, states:

> All WRAMC[44] personnel including military, contractors, students and volunteers are designated as Non-critical sensitive and therefore are required to have a National Agency Check with Local Agency and Credit Checks (NACLC) or ANACI [Access National Agency Check with Inquiries] level of background investigation.

181. TASKORD R101210.01, paragraph 3a(2) states:

> ADP/IT Levels. Pursuant to Reference d.,[45] all personnel assigned to a USN installation who require access to Personal Identifiable Information (PII) are classified as ADP/IT Level II: Non-Critical Sensitive.
>
> Level I: Critical Sensitive Position. Potential for grave to exceptionally grave impact and /or damage.

[43] TASKORD R101210.01 applies to gaining access to the Navy IT network and not the WRNMMC network.

[44] WRAMC refers to the former Walter Reed Army Medical Center; under BRAC, WRAMC and NNMC were combined to establish WRNMMC on 15 September 2011.

[45] SECNAV M-5510.30 (June 2006)

Level II: Non-Critical Sensitive Position. Potential for some to serious impact and/or damage.

Level III: Non-Sensitive Position. Potential for no impact and/or damage as duties have limited relation to the agency mission."

182. JTF CAPMED-I 5210.01 December 13, 2011 states:

1. PURPOSE. This Instruction, in accordance with (IAW) the authority in References (a) through (d) and the guidance in DoD 5200.2-R and DoD 5220.22-R (Reference (e) and (f), implements policy for the Joint Task Force National Capital Region Medical (JTF CapMed) PSP.

2. APPLICABILITY. This instruction applies to JTF CapMed and all Joint Medical Treatment Facilities and Centers in the National Capital Region (i.e., Fort Belvoir Community Hospital, Walter Reed National Military Medical Center, and the Joint Pathology Center).

183. JTF CAPMED-I 5210.01 December 13, 2011, Enclosure 2 paragraph 5c. states:

Through the Joint Personnel Adjudication System (JPAS), verify the clearance status or background investigation determination of new employees to the JTF CapMed or assigned forces command upon arrival. ...As outlined in Reference (e), contractors must have either a fu1ly adjudicated clearance or favorable background investigation determination from a Central Adjudicating Facility (i.e., Office of Personnel Management (OPM), Defense Office of Hearings and Appeals, or Defense Industrial Security Clearance Office) prior to being granted access to Information Technology (IT) level I or II sensitive data. Contractors in sensitive positions may be granted interim access after the background investigation is opened by OPM and the application has been evaluated as an acceptable risk by the PSO.

184. JTF CAPMED-I 5210.01 Incorporating Change 1, April 22, 2013 states:

1. “. . .

2. APPLICABILITY. This Instruction applies to JTF CapMed Headquarters, Fort Belvoir Community Hospital (FBCH), Walter Reed National Military Medical Center (WRNMMC)

[hereafter, FBCH and WRNMMC are referred to as Joint Medical Treatment Facilities (MTFs)], and the Joint Pathology Center.

3. POLICY. It is JTF CapMed policy to implement the procedures established in Reference (e).

4. . . .

5. PSO. The PSO will:

a. Assist the CJTF, Director, J-3A, and the Chief, Security Division with managing the Command's PSP by determining the adequacy of its programs.

b. Verify, monitor, and evaluate all security clearances and background investigation determinations for personnel assigned to or employed by the JTF CapMed, its assigned or attached forces and personnel, and report the status to the CJTF via the chain of command.

c. Through the Joint Personnel Adjudication System (JPAS), verify the clearance status or background investigation determination of new employees to the JTF CapMed or assigned forces command upon arrival. . .. As outlined in Reference (e), contractors must have either a fully adjudicated clearance or favorable background investigation determination from either a DoD Central Adjudicating Facility (DoD CAF), or local adjudicator prior to being granted access to Information Technology (IT) level I or II sensitive data. Military, civilians, and contractors in sensitive positions may be granted interim access after the background investigation is opened by Office of Personnel Management (OPM) and the application has been evaluated as an acceptable risk by the PSO or after a Request for Research and Upgrade has been submitted to the DoD CAF to reevaluate a completed investigation."

185. DoD 5200.2-R, DoD Personnel Security Program, paragraph C3.6.15, states:

C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems

> may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows: (definitions of the types of background investigation cited below can found under the heading “Regulations” in this allegation)
>
> ADP-I: BI
> ADP-II: DNACI /NACI
> ADP-III: NAC /ENTNAC”

186. On 10 February 2012, the Complainant sent an e-mail to Subject 2 and three WRNMMC officials including Complainant’s PSO Coworker; it stated:

> Please review the attached employment contract clause, which I have drafted to forward to HSC [Health Services Contracting Office]. We must move swiftly to ensure that this process is promptly implemented in accordance with the Personnel Security Program outlined by JTF. Please promptly advise as to any recommendations and/or changes. I will like to send this ASAP.

187. Subject 2 testified that, based on the Complainant’s recommendation, he issued a memorandum on 2 February 2012, to the Health Services Contracting Office (HSCO) and Contracting Entities. The subject line was “Employment Contract Clause for Accessing Sensitive/Classified, and/or Access to Sensitive Information Technology Data and Information.” Subject 2 stated the purpose of the memorandum was to draw contracting officials’ attention to the requirements of JTF CAPMED-I 5210.01, which required contracting offices to incorporate a clause into all contracts to define what BI/SC (security clearance) requirements had to be met by the contractor. Subject 2 stated he included a proposed clause with the memo reflecting the requirements of JTF CAPMED-I 5210.01. Subject 2 sent the memo to the Chief of the Logistics Department, WRNMMC, and another member of the Logistics Department, “copy to” former DCO-Admin, WRNMMC. The memorandum stated:

> Security clearances and background investigations and suitability determinations for contract employees are to be submitted and maintained by the contract employee’s FSO at their respective contracting company or agency. The FSO shall also be responsible for initiating reinvestigations as required; thus, ensuring that all background investigations remain current throughout the contract

> performance period. The WRNMMC Personnel Security Office will service the contract employee once all security requirements have been met by the contracting agency; however, the WRNMMC PSO is not responsible for submitting or processing any security clearance or background investigation for contract employees.

188. Subject 2 testified that he signed the memorandum for the HSCO and Contracting Entities to inform them about the new process mandated under JTF CAPMED-I 5210.01. Subject 2 further testified that the memo required contractors to have a BI and the contractors' FSO should initiate the BI. The memo did not mention WRNMMC was also capable of conducting the investigation if the contracting company was not able to conduct it.

189. Subject 2 further testified that the language he used in the memo came from JTF CAPMED-I 5210.01. He also explained that when "PSO" was mentioned, it referred to the WRNMMC PSO. Subject 2 stated the Complainant was solely responsible for conducting the BI/SC determination on all WRNMMC contractor employees, and that the Complainant did not have responsibility for vetting Government civilian employees as others assigned to the PSO were assigned that task.[46]

190. The Complainant is a PSS, who served as the Acting CSM in the WRNMMC PSO beginning in June 2013 when Subject 2 relieved Complainant's PSO Coworker as the CSM. During a meeting on 12 September 2013, Subject 2 gave the Complainant a letter officially assigning him as the CSM then made the decision during the same meeting to rescind the assignment.

191. As stated in JTF CAPMED-I 5210.01, the WRNMMC PSO had responsibility for verifying, monitoring, and evaluating all BI/SC determinations for personnel assigned to or employed by the JTF CapMed, its assigned or attached forces and personnel, and report the status to the CJTF via the chain of command. Based on the Complainant's assigned duties in the PSO office, he was responsible for performing these tasks as they related to contractor employees.

192. The Complainant testified he thought the language in the MedPro contract meant WRNMMC was "supposed to" initiate the BI. The Complainant stated the WRNMMC PSO office was only responsible for checking JPAS to determine whether an

[46] As noted on the sample ITD Check-In Sheet earlier in this report, Complainant's PSO Coworker, who worked with the Complainant in the PSO, was responsible for vetting Government civilian employees.

investigation had been initiated or completed for the contractor employee. He stated WRNMMC had been abiding by the JTF CAPMED "from last year" [April 2013] and that document stated the contractor's Facility Security Officer (FSO) was responsible for assuring their prospective employees had required BIs.

193. The JTF CAPMED-I 5210.01 Incorporating Change 1, April 22, 2013, Enclosure (3) states:

> 1. ACCESS TO INFORMATION. Individuals entrusted with sensitive/classified and/or sensitive IT information must possess a clearance or background investigation determination consistent with the level of access based on the following principles:
>
> a. There is a need for the information in the performance of the assigned task or duty (need-to-know).
>
> b. Appropriate investigative requirements have been met and that these requirements are documented in JPAS.
>
> . . .
>
> (2) Security clearances and background investigation/suitability determinations for contract employees should be submitted and maintained by the contract employee's Facility Security Officer (FSO) at their respective company whenever possible; however, if no FSO is available or is unable to process Positions of Trust, the PSO will submit the background investigation and service the contract employee once all security application requirements have been met by the contracting agency.

194. JTF CAPMED-I 5210.01 states the security clearances and background investigation suitability determinations "should" be submitted and maintained by the contractor employee's FSO, but does not specify the FSO "must" or is required to conduct the suitability determinations or that the Government cannot initiate those suitability determinations.

195. On 7 December 2012, the B.E.A.T Vice President e-mailed the WRNMMC CIO/COR and copied Subject 1. The subject line of the B.E.A.T Vice President's e-mail was "WRNMMC is not processing our NACLCs." The B.E.A.T Vice President stated that B.E.A.T. was in compliance with contract requirements. He also stated that a NACLC is the requirement and the WRNMMC PSO was supposed to initiate the request for the investigation.

196. The B.E.A.T Vice President testified he became aware of the missing security language in the contract when he realized WRNMMC PSO was not processing the BIs. He stated during the time period of the contract, B.E.A.T possessed an Industrial Clearance, DD 254, and their FSO could initiate BIs for their contractor employees. The B.E.A.T Vice President stated that because the contract did not contain the proper clauses the company could not initiate the BIs. The B.E.A.T Vice President further testified that if B.E.A.T. were to have to initiate any BIs without appropriate language in the contract, they could be accused of fraud, waste, and improper use of Government resources. The B.E.A.T Vice President also expressed concern that the Industrial Clearance B.E.A.T. possessed could have been "cancelled."

197. On 11 December 2012, the Complainant e-mailed Subject 1 and informed him that the contract language was "flawed." The Complainant forwarded JTF CAPMED-I 5210.01 to Subject 1 and stated that per the instruction, BI/SC suitability determinations for contractors are submitted and maintained by the contractor's FSO at their respective company; that the WRNMMC PSO will service the contractors once all security requirements have been met by the contracting agency; and that the PSO is not responsible for submitting or processing a BI/SC for contractors.

198. The MedPro, LLC, contract, number W91YTZ-12-C-0157, states, at Section 6.2.3 Contract Officer Representative:

> The COR will be identified by a COR appointment letter. The COR monitors all technical aspects of the contract and assists in contract compliance. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. The COR is not authorized to change any of the terms and conditions of the contract. COR:_WRNMMC CIO/COR email: WRNMMC CIO?COR@amedd.army.mil"

199. Based on the MedPro contract designation of the WRNMMC CIO/COR as the COR, investigators asked the WRNMMC CIO/COR about his efforts to modify the contract. The WRNMMC CIO/COR testified he discovered in September or October of 2012 that the language in the contract was incorrect. The WRNMMC CIO/COR stated that, normally, he would submit a request for a BI to the WRNMMC PSO, the PSO would upload the contractor employee's information in JPAS, and the command would pay for the investigation. According to the WRNMMC CIO/COR, JTF CAPMED was low on funds and would no longer pay for investigations, but the contractor would. The WRNMMC CIO/COR testified it was a "catch 22" situation because JTF CAPMED would not pay for contractor employee BIs and the contract did not require the contractor to pay for it.

200. The WRNMMC CIO/COR stated the ITD requested NARCO add language to the contract consistent with JTF CAPMED-I 5210.01. He said that it took six months for NARCO to issue the modification which contained only the revised labor categories and did not include the revised security language. The WRNMMC CIO/COR testified that since it took NARCO six months to issue the modification, he did not request another modification because the contract period was going to end before a new modification could be issued. He stated that the former DCO-Admin made the decision for WRNMMC to process the BIs and pay for them if the contractor was unable to do it, and this decision would apply to all WRNMMC contracts.

201. On 3 January 2013, the WRNMMC ITD Chief e-mailed the NARCO Contracting Officer in an attempt to modify the contract. The WRNMMC ITD Chief requested the NARCO Contracting Officer modify the MedPro/B.E.A.T. contract and add language that required a Secret Clearance. In response to the request, the NARCO Contracting Officer asked the WRNMMC ITD Chief to strike through sections of the contract and insert proposed changes.

202. On 23 January 2013, the WRNMMC ITD Chief e-mailed the NARCO Contracting Officer, his proposed changes to the security clearance language changing the requirement for a NACLC or NACI to the requirement for onsite contractor employees to have an active "Secret" clearance prior to reporting for duty. The WRNMMC ITD Chief informed the NARCO Contracting Officer that the language in the contract should state that interim clearances for newly-hired personnel shall be processed by the contractors' FSO as expeditiously as possible since contractor personnel will be required to hold "IT-2 positions" and that such clearances must be obtained by the contractor through the Defense

Industrial Security Clearance Office. The WRNMMC ITD Chief testified that contractor employees should have completed a SAAR-N prior to gaining access to the WRNMMC IT network. When asked specifically about Kor Emp 1, the WRNMMC ITD Chief stated he did not know who supervised Kor Emp 1 when he worked as a contractor in the ITD or who would have signed off on Kor Emp 1's SAAR-N form.

203. The former DCO-Admin explained he was responsible for administrative functions at WRNMMC, to include the facilities, HR, logistics, and patient administration. The former DCO-Admin testified the biggest issues he encountered during the transition from the "old Walter Reed to the new" were the clinical contracts for doctors and nurses because WRNMMC was applying a "different level of requirements" than WRAMC. The former DCO-Admin further explained that because WRAMC employees had been cleared under a different set of rules he decided to keep WRAMC personnel working while they attempted to bring the former WRAMC employees' background investigation requirements in line with the new requirements. The former DCO-Admin stated that the process was to allow the employees whose BI check had already been submitted to continue working and upgrade the BIs for those who already had a clearance. The former DCO-Admin testified that he had authority to make the decision to assume the risk and allow contractor employees to remain on the contract. The former DCO-Admin stated he informed the Commander or the Chief of Staff. The former DCO-Admin did not know which regulation gave him the authority to allow the contractor employees to continue working.

204. On 23 January 2013, The former DCO-Admin issued a memorandum for the record, with the subject line: Network Access for Contractors. It stated:

> 1. The Walter Reed National Military Medical Center Commander authorizes the Information Technology Department permission to grant temporary network and administrative rights to employees hired under contract: W91YTZ-12-C-0157 [MedPro/B.E.A.T.].
>
> 2. These rights are granted only in interim to the current contract modification signature approval date. Any employees hired after the approval date is subjected to any security and access requirements stated in the modified contract.

205. On 25 January 2013, the WRNMMC CIO/COR e-mailed The former DCO-Admin's 23 January 2013 memorandum to the WRNMMC ITD Chief, the NARCO Contracting Officer, and another U.S. Army employee. The memorandum stated the WRNMMC Commander authorized the ITD permission to grant the contractors hired under W91YTZ-12-C-0157 temporary network and administrative rights pending contract modification. In the e-mail, The WRNMMC CIO/COR stated the memo references the authority for the IT and Security departments[47] to grant interim domain access pending contract modification.

206. The former DCO-Admin testified Subject 2 would raise concerns during weekly meetings, if there were any, and that Subject 2 would report to him the number of contractor employees, General Schedule employees, and some former Navy personnel, whose background check had been completed each week. The former DCO-Admin had no specific recollection of anyone telling him about 20 IT contractors not having had their BIs.

207. The former DCO-Admin testified that he or the JTF CAPMED Security Division Chief gave the authorization for the WRNMMC PSO to conduct the BIs. The former DCO-Admin further testified that although JTF CAPMED-I 5210.01 stated that the WRNMMC PSO was not responsible for submitting or processing any BIs/SCs for contractors, the instruction did not prohibit the WRNMMC PSO from doing so. The former DCO-Admin also stated he believed he had the authority to waive the background check requirements as failure to accept the risk would negatively impact the WRNMMC mission. The former DCO-Admin stated, "I was certain that I had the authority but I do not recall any written policy that would delegate that authority."

208. The former DCO-Admin stated many contract companies did not have the ability to process BIs and that while JTF CAPMED-I 5210.01 states the WRNMMC PSO was not responsible for submitting or processing BIs/SCs for contractors, the instruction did not prohibit the WRNMMC PSO from submitting or processing them. The former DCO-Admin stated if the contractor could not process their own BIs/SCs, WRNMMC would initiate the process. The former DCO-Admin recalled having many meetings involving the Complainant's interpretation of the regulations; that the Complainant's interpretation was different than Subject 2's and the JTF CAPMED Security Division Chief. The former DCO-Admin stated the Complainant interpreted JTF CAPMED-I 5210-I to mean that WRNMMC was not authorized to initiate the BI/SC process for

[47] According to the WRNMMC organization chart, Subject 2 duties included oversight of the PSO.

contractor employees. The former DCO-Admin testified that he cannot recall authorizing Subject 2 to tell the Complainant to initiate the BIs/SCs process, but believed he did so prior to or on 10 January 2013, the day Subject 2 sent an e-mail to the Complainant stating that from that day forward the Complainant had authorization to process ITD contractor employee BIs until the contractor employees' company had the capability to initiate the BIs.

209. The WRNMMC ITD Chief stated he managed approximately 12,000 employees' computer accounts. The WRNMMC ITD Chief stated he authorized his service chiefs, the WRNMMC CIO/COR, Subject 1, the WRNMMC Chief Information Management Officer, and the WRNMMC IT CTO to grant contractors access to WRNMMC computers using his delegated authority. The WRNMMC ITD Chief stated his service chiefs determined the type of access the contractors required based on the contractors' assigned duties under the contract.

210. The WRNMMC ITD Chief stated the IT contractors completed a Check-in [Profile Sheet] initiated in Subject 2's department to confirm the contractor had a background check. The WRNMMC ITD Chief explained, although the process was not codified anywhere, his understanding was that the contractors presented the Profile Sheet to one of his service chiefs to request access to the WRNMMC network. The WRNMMC ITD Chief stated Subject 2, as the head of the HR department, had no role in granting contractors access to the WRNMMC network.

211. Subject 1 reported to The WRNMMC CIO/COR and was responsible for the MedPro contract One-Stop technicians who assisted WRNMMC staff members to resolve a wide range of IT issues. Subject 1 stated the One-Stop technicians created IT accounts for WRNMMC personnel. Subject 1 also testified that due to mission requirements, leadership made the decision to allow the MedPro/B.E.A.T. contractor employees to have network access, while the contract was being modified, even though the PSO did not sign the SAAR-N form. Subject 1 believed this was the process the One-Stop staff was utilizing based on the guidance received from the WRNMMC ITD Chief and supported by The former DCO-Admins' Memorandum For the Record authorizing interim network access to MedPro/B.E.A.T. contractor employees pending their compliance with BI requirements. Subject 1 stated the Information Assurance Systems Administrator (WRNMMC IASA) in the WRNMMC Information Assurance office filed copies of the SAAR-N forms. The investigators requested the WRNMMC ITD Chief and the WRNMMC IASA provide copies of the SAAR-N forms for any of the

MedPro/B.E.A.T. contractor employees but they did not have any of the MedPro/B.E.A.T. contractor employees' forms in their files.

212. Subject 1 stated that he or another supervisor in the ITD could have granted permission for the contractor employees to access the WRNMMC IT network. Subject 1 did not recall whether he granted such permission for the individuals who reported directly to him. Subject 1 stated the SAAR-N form was the document that he signed when he granted IT network access for a contractor employee. Subject 1 stated that, under normal circumstances, the contractor employee would have had the SAAR-N fully completed and signed before receiving an account; however, in this particular situation, the contract did not contain the appropriate security language so an accommodation was made. Subject 1 stated that due to mission requirements, leadership made the decision to allow the contractor employees to have IT network access, while the contract was being modified, during which time the SAAR-N forms were not signed by the PSO. He said that he was informed of this through his leadership, the WRNMMC ITD Chief, whom he thought probably gained the authority from the former DCO-Admin.

213. The investigators identified 36 contractor employees hired under the MedPro/B.E.A.T. contract. Out of the 36 contractors, the investigators were only able to obtain SSNs for the 27. [48] A JPAS search of the 27 contractor employees revealed that prior to or during the contract period that 17 out of the 27 either had a background investigation that qualified them to be granted a SECRET or TOP SECRET clearance, or either had a NACI or NACLC investigation. The remaining 10 contractor employees had no record of a NACI or NACLC being conducted prior to or during the contract period.

214. The investigators also reviewed the two follow-on STS contracts issued after the MedPro/B.E.A.T contract, for these IT services. Both contracts stated that contractor employees must meet the SC requirement at the beginning of the contract's performance period, and that a minimum active SECRET clearance is required. Our review of JPAS records for the 68 STS contractor employees identified to us under these two contracts showed that 11 of the 68 contractor employees did not have the required SECRET clearance when they began performance, yet were allowed access to the WRNMMC IT network even though they have

[48] In response to investigators' requests for the SSNs, MedPro/B.E.A.T., respecting Privacy Act requirements regarding the former employees, did not provide the remaining SSNs.

yet to complete the vetting process. The review also revealed that 3 currently do not meet the SC requirement.

**Regulations**

215. DoD 5200.2-R, DoD Personnel Security Program, paragraph C3.6.15, states:

> C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows:
>
> ADP-I: BI
> ADP-II: DNACI[49]/NACI[50]
> ADP-III: NAC[51]/ENTNAC[52]

**Discussion and Analysis**

216. The MedPro/B.E.A.T. contract required IT contractor employees to have a NACLC to access ADT/IT-II (AT Level II) information on the WRNMMC network. DoD 5200.2-R requires contractor employees to have a NACI to access ADP-II information on the WRNMMC network.

217. JTF CAPMED–I 5210.01 requires contractors to have either a fully adjudicated clearance or favorable BI determination from a CAF prior to being granted access to IT Level I or II sensitive

[49] DoD National Agency Check Plus Written Inquiries (DNACI): "A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, credit bureau check, and written inquiries to current and former employers…covering a 5-year scope."

[50] National Agency Check Plus Written Inquiries (NACI): A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

[51] National Agency Check (NAC): A personnel security investigation consisting of a records review of certain national agencies…including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

[52] Entrance National Agency Check (ENTNAC): A personnel security investigation scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the FBI is not conducted.

data. The contract that MedPro/B.E.A.T operated under, however, stated in paragraph 5.1.4.1 that all contractor employee positions were ADP/IT-II (IT Level II), Non-critical-Sensitive positions and required a NACLC. We determined 10 of 27 contractor employees that filled the 20 FTE IT positions in the WRNMMC ITD did not have the required BI before they were assigned their duties and had access to IT Level I or II sensitive data. Neither did these 10 have a NACI investigation as required by DoD 5200.2-R, C3.6.15 for contractor employees with ADP-II access. Although the former DCO-Admin authorized temporary access to contractor employees pending the contract modification, we found no evidence that the contractor or any official at WRNMMC attempted to initiate an appropriate background check for any of the contractor employees.

218. We noted that the former DCO-Admin, who testified he was aware the IT contractors did not have BIs/SCs, believed he had the authority to accept the risk of keeping the contractors in place in spite of their lack of proper security screening. We determined, however, that the former DCO-Admin did not have the authority to accept such risk without ensuring a proper background check had been initiated and the PSO had assessed the individual as being an acceptable risk. The ITD failed in their efforts to modify the contract to require a Secret Clearance, so on 10 January 2013, with the former DCO-Admin's support, Subject 2 sent an e-mail to the Complainant stating that from that day forward the Complainant had authorization to process ITD contractor employee BIs until the contractor employees' company had the capability to initiate the BIs. Because Subject 2, the WRNMMC ITD Chief, and the WRNMMC CIO/COR had not been successful in their efforts to obtain a contract modification that included the Complainant's suggested background investigation language, the Complainant refused to process the IT contractor employees' background investigations until WRNMMC modified the contract or provided a letter signed by the Commander authorizing him to do so. The Complainant's decision not to request OPM to initiate BIs for contractor employees contributed to the IT and HR Departments' inability to comply with the requirement that contractor employees have a qualifying BI prior to allowing them access to the WRNMMC IT network. Knowing the Complainant was not conducting the required checks, Subject 2 was responsible for finding someone other than the Complainant to conduct the checks to ensure the contractor employees had undergone the required vetting and screening before they were granted access the WRNMMC IT network.

219. The former DCO-Admin's confusion about his responsibility under the instruction notwithstanding, other key WRNMMC officials identified in this report also failed to take appropriate action in response to the concerns the Complainant raised about contractor employee security clearances and their improper access to the WRNMMC IT network and the information stored therein.

220. We determined that the MedPro/B.E.A.T. contract did not identify the labor category for each IT contractor employee or require the contractor to provide individuals with BIs/SCs. The WRNMMC CIO/COR testified that he requested NARCO modify the MedPro/B.E.A.T. contract and add appropriate language that would list the labor category for each of the 20 FTE positions and require the contractor to provide individuals with qualifying BIs/SCs. We accepted the WRNMMC CIO/COR's testimony on this point but did not understand why he did not follow up with NARCO when NARCO changed the labor categories but failed to include the language about the BIs/SCs in the change they made to the MedPro/B.E.A.T. contract.

221. In e-mails he sent to the NARCO Contracting Officer on 3 and 23 January 2013, the WRNMMC ITD Chief requested NARCO modify the MedPro/B.E.A.T. contract to include language requiring a Secret clearance. We determined like the WRNMMC CIO/COR, the WRNMMC ITD Chief failed to follow up with the NARCO Contracting Officer upon receipt of the contract modification in March 2013 that did not require a Secret clearance. The contract period ended in November 2013, which created a seven month gap during which MedPro/B.E.A.T. contractor employees were never vetted or screened for access to the WRNMMC IT network. The WRNMMC ITD Chief knew that prior to access to the WRNMMC IT network contractor employees had to complete a SAAR-N form which required PSO to conduct a background check. The WRNMMC ITD Chief confirmed contractor employees did not complete the SAAR-N forms prior to gaining access to the WRNMMC IT network because leadership made the decision to allow the contractor employees access pending the completion of their respective background investigations.

222. Subject 1 had responsibility for initiating the SAAR-N form for his 10 Helpdesk FTEs to request approval for his employees' access to the WRNMMC IT network. After receiving the signed SAAR-N form, the PSO was responsible for ensuring the contractor employees had a DNACI or NACI, as required by DoD 5200.2-R for contractor employees. Subject 1's One-Stop Shop, as noted in the ITD Check-In Profile Sheet, was responsible for

establishing contractor's computer accounts, however, the evidence shows Subject 1 reported to The WRNMMC CIO/COR and, therefore, did not have the authority to override the decision his leadership made to waive the completion of SAAR-N forms and background check. Subject 1 followed the direction the WRNMMC ITD Chief, as the ITD CIO, provided to the ITD to continue allowing contractor employees access to the WRNMMC network pending the contract modification based on the former DCO-Admin's memo. Subject 1 was also not in a position to effect the necessary changes to the MedPro/B.E.A.T. contract. The WRNMMC CIO/COR, as the COR on the contract, and the WRNMMC ITD Chief, as the CIO of the ITD, were responsible for ensuring the contract was modified after they received the former DCO-Admin's memo in January 2013.

223. The contract required a NACLC which is a higher-level background check than a NACI. According to DoD 5200.2-R paragraph C3.6.15, the appropriate BI for ADP/IT-II personnel is either a DNACI or a NACI. The investigators concluded 10 MedPro/B.E.A.T. contractor employees did not meet the requirements of DoD 5200.2-R or the MedPro/B.E.A.T. contract

224. Accordingly, we concluded that WRNMMC failed to protect, at a minimum, IT Level II information when contractor employees improperly accessed the WRNMMC IT network during the period of the MedPro/B.E.A.T. contract from September 2012 to November 2013. The contractor employees did not have the requisite BI and PSO did not initiate the administrative process to request the required BIs from OPM as the former DCO-Admin directed in his memo. Thereafter, the ITD granted contractor employees interim access, however, no one followed up to ensure the contract was modified or that the BIs were being processed and, as a result, the contractor employees never received a qualifying investigation in violation of DoD 5200.2-R.

**Conclusion**

225. The allegation is **substantiated**.

**Recommendations**

226. WRNMMC ITD should work with human resources and the contracting officer to determine whether ITD personnel need IT-I or IT-II sensitive information access and comply with the security requirements of DoD 5200.2-R. When determined necessary for IT-I access, contractors must have a BI and an approved SC. WRNMMC ITD should determine whether specific

contractor employees will have access to classified information or critical-sensitive information, and when they will not. The contract will clearly define contractor employee security requirements and require the contractor to bear the cost of BIs. When a SC is required, the contract should hold the contractor responsible to hire and provide only personnel with a previously approved SC or bear the costs of obtaining a SC with a NACLC.

227. WRNMMC and NSAB should suspend base access and information systems privileges of all contractor employees who are determined to be working without interim or permanent security checks. The contracting officer will work with the contractor and NSAB to resolve the deficiency. If contractor employees are found to be non-compliant, recommend WRNMMC officials remove the contractor employees from the contract pending completion of their clearance or have their work duties reduced in scope until their clearance is granted pending compliance with security check procedures.

**Actions Planned or Taken**

228. In January 2012, WRNMMC recognized the IT contract was deficient in failing to require the contractor employees to have a BI and SC. WRNMMC requested NARCO to modify the contract to include this provision, but it took six months for NARCO to issue the modification which did not include the revised security language. The contractor services that were provided in the MedPro contract (W91YTZ-12--0157), are those services now provided via the STS contracts (N00189-14-C-Z004 & N00189-14-C-Z043). The second (current) contract correctly established requirements for contractor employees to comply with qualifications for access to IT systems and for contractors to pay for required contractor BIs/SCs.

229. During the course of this investigation, WRNMMC IG reviewed information about the MedPro/B.E.A.T. contract which expired in November 2013. The contract provided funding for 20 Full Time Equivalent (FTE) positions. Records indicated there where a total of 38 individuals utilized during the course of the contract to meet the missions. One individual was processed but was not called to provide service under the contract. There is no historical record that identifies the level of access that contract personnel are provided after they are removed from the IT system. Personnel are removed at the conclusion of the contract or if/when the individual is no longer providing service under the terms of the current contract. Per interviews, anecdotally, 36 of the individuals were providing help desk

services (answering phones, processing trouble tickets) and, while they were given access to domain accounts via user name and password, the only additional privilege that would have been granted would enable the process trouble tickets that were submitted electronically to the ITD Help Desk Ticket system. Sworn testimony from IT staff indicated that none of the contract personnel associated with the MedPro/B.E.A.T. contract had access to sensitive information, PII. Classified information is not and never has been on the WRNMMC network.

230. The STS contract states that contractors must meet the security clearance requirement at the beginning of contract performance. In August 2014, during the investigation, the investigators suspected some of the contractors on the STS contract have not been in compliance with having a NACLC or a secret clearance as specified in the contract.

a. On 12 August 2014, STS provided a list of the 68 STS contractors along with their SSN, as well as the dates that they started and ended on the contract.

b. On 15 August 2014, WRNMMC IG asked the WRNMMC personnel security office to look in the Joint Personnel Adjudication System (JPAS), for the security clearance status for the 68 personnel.

c. On 18 August 2014, the WRNMMC IG office then forwarded the results to CNIC IG. CNIC confirmed 50 contractors were fully in compliance with the contract; they had the appropriate clearances.

d. On 25 August 2014, CNIC IG office asked the CNIC personnel security office to recheck in JPAS for 18 of the names, as it was not clear if those individuals had met the contract requirement. That day, CNIC IG office provided results showing that seven contractors were in compliance (57 out of 68). Eleven of contractors did not meet the requirement when they started working on the contract. As of 25 August 2014, four of the eleven no longer work as part of the contracts. Out of the remaining seven, four obtained a SECRET or Interim SECRET since working on the contract. Regarding the remaining three individuals, JPAS indicated that one had a pending eligibility, one had a pending SECRET, and the third had opened and closed investigation dates, but no clearance status.

231. Regarding the three STS contractors who have not received an approved interim or finalized secret clearance, WRNMMC notified the contractor of the breach. WRNMMC has taken measures to remove the three individuals from access to WRNMMC systems.

232. Future command decisions concerning new contract personnel will be documented in writing. WRNMMC with NSAB will expedite entering contractor names into the Joint Personnel Adjudication System (JPAS), and requests for background checks (SF86's) will be expediently submitted to OPM for processing.

233. Effective March 2014, DHA took over the contracting function for NCRMD, WRNMMC and FBCH.

**Allegation Four**

Allegation Four: That, pending resolution of a contract dispute, Subject 2, Chief, Human Resources and Manpower, WRNMMC, failed to ensure personnel in the Personnel Security Office who reported to him initiated requests to OPM necessary for contractor employees to obtain the NACLC background investigation contemplated by the contract, before getting access to the WRNMMC IT network.

**Findings of Fact**

234. The Complainant alleged his immediate supervisor, Subject 2, knew that Kor Emp 1 and approximately 20 other MedPro/B.E.A.T. contractor employees did not have a BI/SC, but allowed them to have access to sensitive, classified information or PII on the WRNMMC network.[53] The Complainant stated when he reported the situation to Subject 2 he was under the impression that Subject 2 wanted him to overlook the issue because the contractors would be gone once the contract ended.

235. We found no evidence to support this allegation, but we did find that Subject 2 failed to carry out the former DCO-Admin's direction that, pending modification of the MedPro contract, the PSO take the steps necessary to initiate the process of getting a NACLC, the type of BI contemplated by the contract, for each of the contractor employees working on the MedPro contract.

[53] A total of 36 individuals were identified as MedPro/B.E.A.T contractor employees and they filled, at various times, the 20 FTE positions required under the support contract.

236. The findings of fact for allegation three are incorporated by reference. We repeat some of the findings from allegation three because they are particularly pertinent here.

237. Based on the MedPro contract designation of the WRNMMC CIO/COR as the COR, investigators asked the WRNMMC CIO/COR about his efforts to modify the contract. The WRNMMC CIO/COR testified he discovered in September or October of 2012 that the language in the contract was incorrect. The WRNMMC CIO/COR stated that, normally, he would submit a request for a BI to the WRNMMC PSO, the PSO would upload the contractor employee's information in JPAS, and the command would pay for the investigation. According to the WRNMMC CIO/COR, JTF CAPMED was low on funds and would no longer pay for investigations, but the contractor would pay for them.

238. The MedPro contract dispute appears to have surfaced in early December 2012. On 7 December 2012, the Vice President of B.E.A.T. e-mailed the WRNMMC CIO/COR and copied Subject 1. The subject line of the B.E.A.T Vice President's e-mail was "WRNMMC is not processing our NACLCs." The B.E.A.T Vice President stated that B.E.A.T. was in compliance with contract requirements. He also stated that a NACLC is the requirement and the WRNMMC PSO was supposed to initiate the request for the investigation.

239. The WRNMMC CIO/COR testified that in the case of the MedPro contract it became a "catch 22" situation because JTF CAPMED would not pay for contractor employee BIs and MedPro argued the contract did not require the contractor to pay for it. The WRNMMC CIO/COR said the former DCO-Admin had made the decision for WRNMMC to process contractor employee BIs and pay for them if the contractor was unable to do it, and that decision applied to all WRNMMC contracts.

240. The former DCO-Admin explained he was responsible for administrative functions at WRNMMC, to include the facilities, HR, logistics, and patient administration. The former DCO-Admin believed that he had authority to make the decision to assume the risk and allow contractor employees to remain on the contract, although he did not know which regulation gave him the authority to allow the contractor employees to continue working.

241. The former DCO-Admin also testified that in addition to waving the security check requirements pending execution of the contract modification, he or the JTF CAPMED Security Division Chief, gave the authorization for the WRNMMC PSO to initiate the

process to obtain the NACLC BIs contemplated by the contract. The former DCO-Admin said that although JTF CAPMED-I 5210.01 stated that the WRNMMC PSO was not responsible for submitting or processing any BIs/SCs for contractors, the instruction did not prohibit the WRNMMC PSO from doing so, and he authorized WRNMMC to pay the costs of that effort until the contract could be modified.

242. On 10 January 2013, Subject 2 sent the Complainant and Complainant's PSO Coworker an e-mail giving them permission to initiate the BIs based on the former DCO-Admin's guidance. Subject 2 testified that he did not recall if the Complainant processed the BIs after he received the 10 January 2013 e-mail but Subject 2 believed he asked the Complainant to ensure he was processing or initiating the BIs and the Complainant told him "he would get to it." Subject 2 stated he also told the Complainant in person to conduct the BIs on 10 January 2013, but did not recall sending another e-mail after that date to the Complainant to request he conduct the BIs. Subject 2's email to Complainant, on which he included Complainant's PSO Coworker, the former DCO-Admin, the WRNMMC ITD Chief, and the WRNMMC CIO/COR, states:

> [Complainant], From now on you have authorization to process IT department contractor background investigation until their company have capabilities to do so.

243. On 11 January 2013, Complainant responded to everyone on Subject 2's email, stating:

> Sir, I don't have a clear understanding of your email. Authorization by who (The Office of the Under Secretary of Defense for Intelligence (OUSD(I)), The Deputy Under Secretary of the Navy, Plans, Policy> Oversight and Integration (N09N2), etc.)? In addition, the [ITD] has several contracts. To my knowledge, all the agencies have Facility Security Officers and are initiating and maintain the investigations for their respective contract employees or have the capability to do so. Please provide additional information. Thank you.

244. When Subject 2 responded, specifically asking the WRNMMC ITD Chief and The WRNMMC CIO/COR which contractors did not have the capability to process background investigations, the WRNMMC ITD Chief responded to all in the email string by stating:

> MedPros, BEAT, and DSG do not have FSOs.

245. Later in the morning of the 11th, Subject 2, closed out the email string on this matter by sending an email to everyone that said:

> ... [Complainant], please lets work on a solution.

246. The former DCO-Admin testified that he cannot recall authorizing Subject 2 to tell the Complainant to initiate the BIs/SCs process, but believed he did so prior to or on 10 January 2013, the day Subject 2 sent an e-mail to the Complainant stating that from that day forward the Complainant had authorization to process ITD contractor employee BIs until the contractor employees' company had the capability to initiate the BIs.

247. On 23 January 2013, the former DCO-Admin issued a memorandum for the record, with the subject line: Network Access for Contractors. It stated:

> 1. The Walter Reed National Military Medical Center Commander authorizes the Information Technology Department permission to grant temporary network and administrative rights to employees hired under contract: W91YTZ-12-C-0157 [MedPro/B.E.A.T.].
>
> 2. These rights are granted only in interim to the current contract modification signature approval date. Any employees hired after the approval date is subjected to any security and access requirements stated in the modified contract.

248. The former DCO-Admin stated many contractors do not have the ability to process BIs and that while JTF CAPMED-I 5210.01 states the WRNMMC PSO was not responsible for submitting or processing BIs/SCs for contractors, the instruction did not prohibit the WRNMMC PSO from submitting or processing them. The former DCO-Admin stated if the contractor could not process their own BIs/SCs, WRNMMC would initiate the process.

249. The former DCO-Admin recalled having many meetings involving the Complainant's interpretation of the regulations; that the Complainant's interpretation was different than Subject 2's and the JTF CAPMED Security Division Chief. The former DCO-Admin stated the Complainant interpreted JTF CAPMED-I 5210-I to mean that WRNMMC was not authorized to initiate the BI/SC process for contractor employees.

250. The former DCO-Admin testified Subject 2 would raise concerns, if there were any, during weekly meetings and that Subject 2 would report to him the number of contractor employees, General Schedule employees, and some former Navy personnel, whose background check had been completed each week. The former DCO-Admin had no specific recollection of anyone telling him about 20 IT contractors not having had their BIs.

251. Subject 2, as the former Chief, HR and Manpower, WRNMMC, was responsible for oversight of the PSO WRNMMC.[54] He stated his responsibilities did not include authorizing contractors' access to WRNMMC computers or IT systems. Subject 2 suggested the investigators contact the WRNMMC ITD Chief, CIO, ITD, WRNMMC, to determine who gave IT contractors WRNMMC computer access. Subject 2 stated the Complainant was responsible for the Check-In process at the PSO and that the contractor employees would report to the Complainant to have him conduct the necessary check in JPAS for the BI/SC information.

252. Subject 2 testified that all WRNMMC personnel, including contractors, go through the same process of checking into the command. He said he believed the contractor employees were required to check-in with the PSO before the ITD provided access to the network.

253. In response to investigator's question as to whether he directed or ordered the Complainant or anyone else in the PSO to initiate the BIs, Subject 2 stated he told the Complainant in person and sent the Complainant and Complainant's PSO Coworker an e-mail giving them permission to initiate the request to OPM for the BIs based on the former DCO-Admin's guidance.

254. The investigators asked Subject 2 if he at any time delegated the task of performing the BIs on contractor employees to anyone else and he stated he did not because the Complainant insisted only he could "deal with contractors" because he was an expert on contractor employees' SCs.

255. Subject 2 stated he did not remember if the Complainant processed the BIs after he received the 10 January 2013 e-mail but he believed he asked the Complainant to ensure he was processing or initiating the BIs and the Complainant told him "he would get to it." Subject 2 stated he also told the Complainant in person to conduct the BIs on 10 January 2013, but

[54] Subject 2 is currently assigned to the Bureau of Medicine and Surgery.

did not recall sending another e-mail after that date to the Complainant to request he conduct the BIs.

256. Subject 2 stated he did not recall a conversation with the Complainant specifically about 20 contractor employees not having a BI/SC. He further stated he did not specifically recall telling the Complainant to overlook the fact that the contractor employees did not have the required BIs; he stated he asked the Complainant to work with the ITD toward a solution.

257. In a follow-up interview, an investigator asked Subject 2 to describe the process for getting a NACLC, with emphasis on what actions the Complainant would take in the PSO. Subject 2 stated that the contractor employees had to complete their background investigative paperwork, and provide it to the Complainant, who would then submit the paperwork electronically into JPAS. Subject 2 stated that the Complainant did not have to contact OPM directly, explaining that once the paperwork was in JPAS, OPM was automatically notified that the paperwork is in the queue for OPM to start processing and begin the required type of background investigation. After the investigation is completed, the results go to the CAF, and the CAF does the adjudication.

**Regulations**

258. We cited no regulations as standards for this allegation and hence there are no regulations to discuss. The issue here is simply whether Subject 2 exercised sufficient diligence to carry out The DCO Admin's intent that WRNNMC, acting through the PSO that reported to Subject 2, initiate the process required for MedPro contractor employees to obtain a NACLC, the BI contemplated by the contract, at WRNMMC expense, pending issuance of the contract modification.

**Discussion and Analysis**

259. JTF CAPMED–I 5210.01 assigned responsibility to the PSOs to verify the security clearance status or BI determination of new employees. We determined Subject 2, as the Chief, HR and Manpower, WRNMMC, was responsible for oversight of the WRNMMC PSO and the check-in process as it related to determining whether contractor employees had a requisite BI.

260. With the authorization of the DCO Admin, Subject 2 requested the Complainant develop a solution in collaboration with the ITD and ensure background checks were properly processed. Subject 2 was responsible to provide appropriate

oversight of the PSO; he was also responsible to ensure the screening process for contractor employees seeking access to WRNMMC networks was completed.

261. We discovered during this investigation that the background checks WRNMMC management officials believed their staff had done or were doing while the contractor employees continued to access the WRNMMC network pending modification of the contract were, in fact, never initiated. The Complainant's refusal to enter information in JPAS for contractor employee BIs, coupled with management's failure to ensure someone assigned to the PSO entered this information into JPAS to allow to OPM conduct a contractor employee's BI were the primary causes of the failure to obtain the NACLC for these employees between January 2013, when the DCO Admin authorized the PSO to initiate the request for the BIs, to November 2013 when the MedPro/B.E.A.T. contract period ended.

262. In this regard, we determined that Subject 2 did not take appropriate measures to ensure the PSO staff initiated the BIs in response to the DCO Admin's clear direction to do so in the interim awaiting the contract modification. With the knowledge that the contract modification did not occur shortly after the DCO Admin sent his memo out in January 2013, it was incumbent upon Subject 2 to direct the Complainant or someone else in the PSO to process the contractor employees for a BI given the risks and potential mission failure associated with allowing non-vetted, unscreened contractor employees to access the WRNMMC IT network more than nine months after the DCO Admin wrote the memo outlining his expectations.

263. We concluded, therefore, that Subject 2 failed in his responsibility, as the Chief of the HR and Manpower Department with oversight of the PSO office, to ensure MedPro/B.E.A.T. contractor employees were properly vetted in JPAS pending the contract modification, as specified in the DCO Admin's 31 January 2013 memo, and that contractor employees were processed for a NACLC, the BI contemplated by the contract.

**Conclusion**

264. The allegation is **substantiated**.

**Recommendations**

265. WRNMMC HR should coordinate with the WRNMMC PSO and NSAB to expedite security checks of all contractor personnel, report

on progress of onboarding contractors, and employees, and serve notice of serious criminal violations, etc.

**Actions Planned or Taken**

266. WRNMMC HR will increase oversight over onboarding procedures and coordinate with NSAB on executing security requirements that are within the control of the WRNMMC.

267. The WRNMMC onboarding checklist was revised in June 2014, and is currently used by the ITD to in-process WRNMMC civilian and contractor employees. The checklist requires the employee to go to each office in the order listed to eliminate the possibility of bypassing an office. The WRNMMC personnel security office (PSO) is on the list and the checklist has a block to check once the PSO completes the security check.

268. WRNMMC will focus on ways to expedite onboarding procedures of all employees to satisfy critical mission needs.

**Allegation Five**

> That, between September 2012 and November 2013, Subject 3, Chief Operations Officer, IT Department, WRNMMC, allowed Kor Emp 1 access to WRNMMC IT systems without first obtaining the results of a National Agency Check (NAC), in violation of DoD policy established in DoD 5200.2-R, DoD Personnel Security Program.

**Findings of Fact**

269. The Complainant alleged that approximately 20 contractors were given improper access to sensitive, classified information or PII, but only identified Kor Emp 1 by name.

270. The Complainant also alleged that Kor Emp 1 was improperly granted administrative rights to the WRNMMC IT system in connection with his duties as the Program Manager and that he had the ability to access any computer on the WRNMMC IT network. The Complainant testified he had “no idea” who provided Kor Emp 1 with access rights but implied Subject 3 was responsible. He said that Subject 3 and those working under him were responsible for network administration. The Complainant further alleged that Kor Emp 1 told the Complainant that he (Kor Emp 1) in-processed to the WRNMMC on 4 December 2012, and bypassed the WRNMMC PSO with the aid of Subject 3.

271. As the COO, Subject 3 was responsible and provided oversight of the operations of the One-Stop Help Desk for IT issues involving WRNMMC staff.

272. On 7 December 2012, Subject 3 wrote an e-mail to the Complainant with the subject line "Meeting with the WRNMMC ITD Chief" and stated:

> Can you kindly coordinate a time with [**the Executive Assistance for the** WRNMMC ITD Chief] to meet with our CIO, the WRNMMC ITD Chief, to discuss our current contracts and the clearance requirements within ITD. I understand Subject 2 has already briefed you on this.

273. In his e-mail reply to Subject 3, on 11 December 2012, the Complainant informed Subject 3 that the MedPro contract language was "flawed." The Complainant forwarded a copy of the JTF CAPMED-I 5210.01 to Subject 3 and noted in his email that according to the instruction, the contractor's FSO was responsible to conduct BI/SC suitability determinations for contractor employees and the PSO serviced the contractor employee once all security requirements had been met by the contractor. The Complainant also stated that the PSO was not responsible for submitting a request for or processing a BI/SC for contractor employees. The Complainant also wrote:

> I'm not sure as to who vetted the flawed contract language in your existing contract; however, I can confirm that it was not our office. Unfortunately, the majority of my work is time sensitive, which leaves me with little to no availability; however, if the WRNMMC ITD Chief still desires to meet after reviewing the attached instruction please advise.

274. Subject 3 forwarded the Complainant's 11 December 2012 e-mail to the WRNMMC ITD Chief and copied Subject 2, Complainant's PSO Coworker, and the WRNMMC CIO/COR. Subject 3 directed the WRNMMC ITD Chief' attention to the Complainant's comments in the e-mail string he forwarded.

275. On 3 January 2013, the WRNMMC ITD Chief e-mailed the NARCO Contracting Officer in an attempt to modify the contract. The WRNMMC ITD Chief requested the NARCO Contracting Officer modify the MedPro/B.E.A.T. contract and add language that required contractor employees to have a SC.

276. On 10 January 2013, Subject 2 sent the Complainant and Complainant's PSO Coworker an e-mail giving them permission to

initiate the BIs based on the DCO Admin's guidance. Subject 2 testified that he did not recall if the Complainant processed the BIs after he sent the complainant his 10 January 2013 e-mail but Subject 2 believed he asked the Complainant to ensure he was processing or initiating the BIs. Subject 2 recalled that the Complainant told him "he would get to it." Subject 2 stated he also told the Complainant in person to conduct the BIs on 10 January 2013, but did not recall sending another e-mail after that date to the Complainant to request he conduct the BIs.

277. On 23 January 2013, the DCO Admin, issued a memorandum for the record authorizing the ITD permission to grant temporary network and administrative rights to MedPro/B.E.A.T. contractor employees. The DCO Admin granted contractor employees interim access pending a modification to the MedPro/B.E.A.T. contract that would require the contractor to initiate the necessary BIs for contractor employees to ensure compliance with the applicable security and access requirements stated in the modified contract.

278. On 23 January 2013, the WRNMMC ITD Chief e-mailed the NARCO Contracting Officer his proposed changes to the security clearance language changing the requirement for a NACLC or NACI to the requirement for onsite contractor employees to have an active "Secret" clearance prior to reporting for duty. The WRNMMC ITD Chief informed the NARCO Contracting Officer that the language in the contract should state that interim clearances for newly-hired personnel shall be processed by the contractors' FSO as expeditiously as possible since contractor personnel will be required to hold "IT-2 positions" and that such clearances must be obtained by the contractor through the Defense Industrial Security Clearance Office.

279. The WRNMMC ITD Chief testified that contractor employees should have completed a SAAR-N prior to gaining access to the WRNMMC IT network. When asked specifically about SubK Emp1, the WRNMMC ITD Chief stated he did not know who supervised Kor Emp 1 when he worked as a contractor employee in the ITD or who would have signed off on Kor Emp 1's SAAR-N form.

280. On 25 January 2013, the WRNMMC CIO/COR e-mailed the DCO Admin's 23 January 2013 memorandum to the WRNMMC ITD Chief, the NARCO Contracting Officer, and another Army employee. In the e-mail, the WRNMMC CIO/COR stated the memo provided the authority for the IT and Security departments to grant interim domain access to contractor employees pending contract modification.

281. In other e-mails he sent to the NARCO Contracting Officer on 3 and 23 January 2013, the WRNMMC ITD Chief requested NARCO modify the MedPro/B.E.A.T. contract to include language requiring a SC. We determined like the WRNMMC CIO/COR, The WRNMMC ITD Chief failed to follow up with the NARCO Contracting Officer upon receipt of the contract modification in March 2013; the modified contract did not include language that required contractor employees to hold a Secret clearance.

282. On 29 August 2013, Subject 3, the WRNMMC IASA, the WRNMMC CIO/COR, and the WRNMMC IT CTO began exchanging e-mails regarding a CAC request for a B.E.A.T. employee, Kor Emp 2. During their 29 August 2013 e-mail exchange, Subject 3 stated that he was "adding [misspelled name of Kor Emp 1] to the string for SA."

283. After being copied on Subject 3's 29 August 2013 e-mail, Kor Emp 1 sent a reply e-mail on 30 August 2013, to the WRNMMC IASA, Subject 1, the WRNMMC CIO/COR, and the WRNMMC IT CTO, and stated: "Greetings, I spoke with the [Complainant] yesterday and provided [him] a copy of Kor Emp 2's ITD in-processing form. The [Complainant] said he would look into this."

284. On 9 September 2013, the Complainant e-mailed Subject 3, regarding the CAC Request for Kor Emp 2 and stated:

> Subject 1,
>
> 1. Your contract employee's name is Kor Emp 1 not [different but similar name].
>
> 2. The ITD Trusted Agent was notified by our office on Fri 8/30/2013 10:46AM that the TASS Request for an initial CAC issuance for was approved, which was 2 Hours 26 Minutes prior to your e-mail inquiry.
>
> 3. The WRNMMC IT CTO was named as a point of reference, as the WRNMMC IT CTO is the only ITD COR our office has a rapport with.
>
> 4. What you and your staff members lookup in JPAS has no relevance and/or effect as to what decisions our office makes; thus, based on your remarks, you and your staff members may potentially be in violation of DoD Regulations governing JPAS.
>
> 5. Kor Emp 1 has not been properly vetted nor does he have a favorable background investigation and/or eligibility to

> be employed on the Federal contract endeavor as an ITD Program Manager. Additionally, ITD has given Kor Emp 1 access to the WRNMMCAMED Network and entrusted him with other ITD employees Personally Identifiable Information (PII), which is to be protected under the Privacy Act of 1974. The necessary action(s) are being taken to address the security concerns and/or violations.

285. On 9 September 2013, Subject 3 replied to the Complainant's e-mail and stated:

> Appreciate the correction on item number 1 as that appears to be a significant and relevant factor in this string, so thank you. At the risk of sounding redundant and going through this all over again, we went through this with the DCO Admin, Subject 2, and I believe we should go through it again with the WRNMMC Director of Administration on this specific set up with one of our staffing contracts. While you may have a rapport with the WRNMMC IT CTO, he is not the COR for the B.E.A.T. contract, thus you will need to establish a rapport with the WRNMMC CIO/COR who is our Deputy CIO (Assistant DH). Just so you are aware, our BEAT contract does not have an FSO at the moment, so it was decided by the DCO Admin (DCA - Senior Leadership) at the time that your department would process these [contractor employees] until such time in the new FY that we made a modification in the contract so that they could process their own [contractor employees]. With that said, this email string appears to be unproductive, so it may be best to set up a meeting with your leadership to discuss the way forward again so that everyone is clear and on the same page.

286. Continuing their e-mail exchange on 9 September 2013, the Complainant wrote back to Subject 3 and stated:

> Thank you for your recommendation; however, I have spoken and it is not required that I meet with anyone related to the noted security concerns and/or violations. Please be advised that a higher authority establishes National Security protocol and DoD Regulations. As stated in my previous email, the necessary action(s) are being taken to address the security concerns and/or violations.

287. Later the same day, on 9 September 2013, Subject 2 e-mailed the Complainant about the e-mail exchange he had with Subject 3 regarding the CAC Request for Kor Emp 2 and stated:

"Please tell me that you did not [take] this outside of our chain?"

288. When we interviewed the Complainant, we asked for his interpretation of the acronym "SA." The Complainant testified he believed "SA" stood for "System Administration." The Complainant acknowledged awareness of the term "situational awareness" but he explained that when he wanted to express this term as an acronym he always included "for" within the abbreviation, such as "FSA" (for situational awareness). The Complainant further testified he primarily focused on the word "Adding" in Subject 3's e-mail statement, "Adding Kor Emp 1 to the string for SA." The Complainant believed that this word choice meant that Kor Emp 1, whom the Complainant believed encumbered an IT Level I or IT Level II sensitive position had the higher level of access associated with those IT Levels, System Administrator, and, therefore, represented an immediate "potential for grave to exceptionally grave impact and/or damage" or a "potential for some serious impact and/or damage" as defined in TASKORD R101210.01.

289. The WRNMMC ITD Chief testified that if Kor Emp 1 had an e-mail address, then it would mean that he had a network account, and would have had a background check (NCIC) conducted by NSAB security, a criminal record check. He stated that Kor Emp 1 would not need to have access across domains or access to shared folders. The WRNMMC ITD Chief stated the individual who provided Kor Emp 1 the account would have been someone who worked the ITD Helpdesk the day Kor Emp 1 checked-in. The WRNMMC ITD Chief further stated that it was unlikely that the logs still existed showing Kor Emp 1's access but, if they did, Subject 3 would be able to provide the information.

290. Subject 3 testified that he did not supervise Kor Emp 1. He believed Kor Emp 1 had to report to a Government employee and that would have been the COR for the MedPro/B.E.A.T. contract, the WRNMMC CIO/COR. The WRNMMC CIO/COR told investigators during follow-up questioning that Kor Emp 1 "checked in with [him] on a daily basis;" but moreover, that it was "probably" he (the WRNMMC CIO/COR) who signed Kor Emp 1's SAAR-N form on the "supervisor line." Subject 3 said that he did not recall who in-processed Kor Emp 1 when he arrived as a new contractor employee but he was never granted IT system administrative rights to the WRNMMC IT network. Subject 3 explained that Kor Emp 1 did not have IT-I or an IT-II level access and he did not encumber an IT-I or an IT-II level position. He said that Kor Emp 1 was the onsite MedPro contract PM and as the PM he did not

perform the duties of a Helpdesk technician and did not require anything other than a regular user domain account to perform his official duties.

291. Subject 3 testified that Kor Emp 1's duties as PM consisted of ensuring personnel staffing requirements related to the contract were met. In this role, Kor Emp 1 did not have access to any IT applications that would give him unauthorized access to Government employee PII or any WRNMMC patient's Public Health Information. Subject 3 said he did not know if Kor Emp 1's position required a BI or SC. He also testified, however, that he believed Kor Emp 1 required the same BI that any command user would require to gain access to the WRNMMC IT network.

292. Regarding ITD records, Subject 3 testified that ITD technicians deleted user access logs 90 days after an account became inactive. In this process, any record about account creation was also deleted. Subject 3 also testified that he did not recall if the MedPro/B.E.A.T contractor employees completed SAAR-N forms during the period of the contract. Subject 3 stated the WRNMMC ITD Chief and the WRNMMC CIO/COR informed him in October 2012 that there was a problem with the contract security language and the contractor employees did not meet the requirement. Subject 3 stated the WRNMMC ITD Chief told him to create the contractor employees' accounts for access to the IT network, while they addressed the contract issue. Subject 3 testified that typically the ITD would need a SAAR-N completed before establishing an account, but that he (Subject 3) was told to give contractor employees accounts prior to completion of the SAAR-N forms. Subject 3 stated he did not know if the ITD had any MedPro/B.E.A.T. completed SAAR-N forms on file but that the WRNMMC IASA, Information Assurance Officer, ITD, WRNMMC, was responsible for maintaining the forms.

293. Subject 3 testified that a Government employee or contractor employee "could" have created a user account for the other contractor employees. Subject 3 stated that during the period of the MedPro contract the WRNMMC Help Desk Branch Chief, reported directly to him and that the Help Desk technicians reported directly to the Branch Chief. Subject 3 testified that due to mission requirements and because the contract had to be modified, technicians created contractor employees' user accounts even though the SAAR-N forms were not completed and signed.

294. Subject 3 stated the ITD check-in sheet did not have to be "signed off" before an account could be created. He said the

SAAR-N form was all that was needed to create the account. Subject 3 stated the check-in sheet was obtained from and turned into DHMRSi.

295. Subject 3 stated that prior to receipt of the DCO Admin's 23 January 2013 memo, WRNMMC leadership discussed modifications to the contract and that the DCO Admin's memorandum was a way of finally documenting leadership's decision to allow contractor employees who did not possess the requisite BI or SC access to the WRNMMC IT network pending the modification of the contract.

**Regulations**

296. DoD 5200.2-R, DoD Personnel Security Program, paragraph C3.6.15, states:

> C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows:
>
> ADP-I: BI
>
> ADP-II: DNACI/NACI
>
> ADP-III: NAC/ENTNAC"

**Discussion and Analysis**

297. This investigation found no evidence to support the allegation that Subject 1 granted Kor Emp 1 access to WRNMMC IT systems as alleged. The testimony we collected established that, although Subject 3 authorized his 10 Helpdesk FTEs access to the WRNMMC IT network, Kor Emp 1 did not work for Subject 1 and Subject 3 was not responsible for approving Kor Emp 1's IT system access. Because of the nature of Kor Emp 1's PM duties and the WRNMMC CIO/COR's recollection about his supervisory role toward Kor Emp 1, we determined that Kor Emp 1 reported to the WRNMMC CIO/COR not to Subject 3. Documentary evidence that would corroborate the witness testimony we collected and show exactly who affected Kor Emp 1's access was apparently destroyed 90 days after Kor Emp 1's IT account became inactive in accordance with ITD standard operating procedure. The lack of corroborating documentary evidence notwithstanding, we found Subject 3 and the WRNMMC CIO/COR forthcoming during their

interviews and follow-up questioning and believed their account of events.

298. We also determined the Complainant mistakenly believed that Kor Emp 1 had been granted system administrator privileges when he had not been. The Complainant's misunderstanding stemmed from his reading of an e-mail that Subject 3 sent on 29 August 2013 wherein he stated that he was adding Kor Emp 1 to the e-mail discussion for his "SA". The Complainant misunderstood the term to mean Subject 3 had given Kor Emp 1 system administrator (SA) rights, but we determined that was not the case.

299. We noted that the DCO Admin made the decision to waive the requirement for the MedPro/B.E.A.T. contractors to access the WRNMMC network pending the contract modification. We also noted that Subject 2 engaged with the contracting officer and attempted to have the existing contract modified in line with the DCO Admin's waiver expectations. Based on the DCO Admin's waiver memo, the WRNMMC ITD Chief, as CIO, made the decision that contractor employees were not required to complete SAAR-N forms pending the contract modification; however, the WRNMMC ITD Chief did not follow through or track efforts to modify the contract. Instead, he allowed contractor employees continued access to ADP-II level information on the WRNMMC network. We determined, therefore, that the contractor employees, including Kor Emp 1, continued improper access to the WRNMMC IT network was a result of the WRNMMC ITD Chief, the WRNMMC CIO/COR and Subject 2 failures to act.

300. We further determined that Kor Emp 1's PM duties only required that he have a "domain account" that provided him with minimal access to WRNMMC's computer network and e-mail access. Although we determined the Complainant was mistaken in his belief that Subject 3 granted Kor Emp 1 improper system administrator privileges, we also determined that Kor Emp 1 was assigned to a non-sensitive IT Level III position as PM. Accordingly, in accordance with DoD 5200.2-R, Kor Emp 1 should have undergone a NAC background investigation but the PSO did not initiate the requisite BI when he was directed to do so.

301. In consideration of the foregoing and by a preponderance of the available evidence, we concluded that Subject 3 did not violate DoD 5200.2-R; Subject 1 had no role in the decision to allow Kor Emp 1 access to the WRNMMC IT network.

**Conclusion**

302. The allegation is **not substantiated**.

**Allegation Six**

That, from September 2012 to November 2013, WRNMMC failed to correct violations of DoD policy established in DoD 5200.2-R, DoD Personnel Security Program.

**Findings of Fact**

303. The discussions throughout this report regarding WRNMMC's actions are incorporated by reference.

304. The Complainant alleged he notified Subject 2 and Subject 3 at various times regarding his concerns that certain WRNMMC contractors did not have a qualifying BI or SC and were, therefore, improperly provided access to WRNMMC IT systems and the sensitive and classified information processed on the WRNMMC IT network. The Complainant further alleged that in response to his notifications, the management officials he contacted failed to take appropriate corrective action. We note here, as was previously documented in this report, the contractors could not have accessed any classified information; classified information was not processed on the WRNMMC IT systems to which the contractors in question were granted improper access.

305. DoD 5200.2-R provides for IT contractor employees who have a DNACI or NACI to access ADP-II information. WRNMMC officials took steps to comply with DoD 5200.2-R C3.6.15., however, as determined in earlier allegations of this report, 10 of the IT contractor employees who performed work on the MedPro/B.E.A.T. contract did not have a NACI, as required, prior to the contract period and were not vetted or screened during the contract period. In January 2013, the DCO Admin authorized the ITD to allow contractors interim access while awaiting completion of their background investigations, and BG Clark represented these investigations were being done in his response to SECDEF in October 2013.

306. Although the DCO Admin testified that he did not recall any contractor employee SC or access issues being raised to him about the WRNMMC ITD, on 23 January 2013, he issued a memorandum for the record granting the MedPro/B.E.A.T. contractors temporary network and administrative rights. The DCO Admin issued this memorandum to address the Complainant's concern that contractor employees continued to access the WRNMMC IT network

without being properly vetted, believing his ITD department head, the WRNMMC ITD Chief, were taking steps to modify the MedPro/B.E.A.T. contract, and Subject 2 was ensuring PSO personnel initiated requests to OPM to conduct the BIs.

307. It appears the DCO Admin and others who relied on the JTF CAPMED-I 5210.01 to allow contractors interim access to ADP-II positions, did so in error. While the language in DoD 5200.2-R in paragraph C.3.2.1 provided an exception for civilian employees to work in noncritical sensitive positions to work in an emergency, that provision does not apply to contractor personnel as it comes under the general heading of civilian employees.

308. 5200.2-R paragraph C3.2. CIVILIAN EMPLOYMENT states:

> C3.2.1. General. The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

309. 5200.2-R paragraph C3.2.5. Exceptions states:

> C3.2.5.1. Noncritical-sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

310. We noted that JTF CAPMED–I 5210.01 of April 22, 2013, Personnel Security Program, references the DoD 5200.2-R and states in enclosure 2, paragraph 5(c), in pertinent part "Military, civilians, and contractors in sensitive positions may be granted interim access after the background investigation is opened by Office of Personnel Management (OPM) and the application has been evaluated as an acceptable risk by the PSO or after a Request for Research and Upgrade has been submitted to the DoD CAF to reevaluate a completed investigation," is inconsistent with the DoD 5200.2-R and may have contributed to WRNMMC management officials' mistaken belief that they had authority to grant interim access.

311. Enclosure 2, paragraph 5(c) JTF CAPMED-I 5210.01 of December 13, 2011, which was also in effect during the

MedPro/B.E.A.T contract period, references DoD 5200.2-R and states “contractors must have either a fully adjudicated clearance or favorable background investigation determination from a Central Adjudicating Facility (i.e., Office of Personnel Management (OPM), Defense Office of Hearings and Appeals, or Defense Industrial Security Clearance Office) prior to being granted access to Information Technology (IT) level I or II sensitive data. Contractors in sensitive positions may be granted interim access after the background investigation is opened by OPM and the application has been evaluated as an acceptable risk by the PSO.” This paragraph in the JTF CAPMED-I 5210.01, referenced the DoD 5200.2-R and is also inconsistent with the DoD 5200.2-R as there is no provision in the regulation to waive the requirement for a contractor employee to have the NACI during the period of work performed.

312. We concluded Subject 2 failed in his responsibilities as the Chief of HR and Manpower to ensure one of his divisions, the PSO, to which the Complainant was assigned, followed established procedures to ensure Kor Emp 1 and other MedPro/B.E.A.T. contractor employees had been properly vetted and screened prior to access to the WRNMMC network. Due to the DCO Admin’s purported waiver of the requirement for the contractor employee to have a completed background investigation, MedPro/B.E.A.T. contractor employees gained access to the WRNMMC IT network throughout the contract period absent a NACI as required by DoD 5200.2-R.

313. In a 9 September 2013 e-mail to Subject 3, the Complainant stated that Kor Emp 1 was not properly vetted. Subject 3’s response to the Complainant was that the DCO Admin had determined the contractors would be granted access to perform their official duties on the WRNMMC IT network until a modification could be made to the contract. In Subject 3’s response to the Complainant, he requested the Complainant set up a meeting with the Complainant’s leadership to address the matter; however, the Complainant declined to participate in the requested meeting.

314. In our introduction to this report, we identified an instance when WRNMMC responded to an earlier complaint raised by the Complainant to SECDEF. We noted that on 23 October 2013, the Director, WRNMMC wrote a letter to SECDEF and acknowledged that WRNMMC was aware that the contract for IT support then in existence was defective and allowed contractors to gain improper access to the network without having completed proper background investigations.

315. In his letter to SECDEF, the Director, WRNMMC reported that the situation the Complainant raised had been identified earlier that year and the next IT contract, effective November 2013, would include the background check requirement omitted in the previous IT support contract. The Director, WRNMMC also stated in his letter to SECDEF that when this situation was first recognized, WRNMMC took steps to limit contractor employees' access and assigned credentialed personnel to supervise them. We discovered during this investigation that the Director, WRNMMC and the DCO Admin believed the WRNMMC staff was initiating requests in JPAS for OPM to conduct the BI during the period the contractor employees had been granted interim access to the WRNMMC network. Complainant's refusal to initiate the requests for the BIs does not excuse the DCO Admin's and Subject 2's inaction in failing to ensure someone assigned to the PSO initiated the request in JPAS to alert OPM to conduct the BI during the period of the MedPro/B.E.A.T. contract.

316. WRNMMC addressed the problems associated with the MedPro/B.E.A.T. contract in the subsequent contract awarded to STS to continue the IT services provided in the MedPro/B.E.A.T. contract (W91YTZ-12-C-Z043). The two STS contracts were N00189-14-C-Z004, awarded on 13 November 2013, with the period of performance ending 31 July 2014; and, contract N00189-14-C-Z043, awarded on 24 July 2014, with the period of performance ending 31 December 2014. Both contracts contained the following language and specifically addressed the problem the Complainant noted with the MedPro/B.E.A.T. contract they replaced:

> All military, Government civilian, consultants, and contractors, who design, develop, operate, or maintain a Network shall possess appropriate clearances and authorizations for access to system components, output, or documentation.
>
> Individual personnel must meet the Security Clearance requirement at the beginning performance under this contract. Minimum active SECRET clearance is required for all Contractors under this contract.

**Regulations**

317. DoD 5200.2-R, DoD Personnel Security Program, paragraph C3.6.15, states:

> C3.6.15. Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II and ADP-III. DoD military,

civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix 10) and investigated as follows:

ADP-I: BI

ADP-II: DNACI /NACI

ADP-III: NAC /ENTNAC”

**Discussion and Analysis**

318. During his interview, the Complainant gave specific examples of having contacted management officials who did not respond to him. We interviewed the management officials the Complainant identified and others we identified as having knowledge of the same issues. Thereafter, we determined what action, if any, those officials took.

319. While we previously identified the cumulative failures of the DCO Admin, the WRNMMC ITD Chief, and the WRNMMC CIO/COR in Allegation Three, and Subject 2’s individual failures in Allegation Four, we noted in mitigation of their respective failures that they proactively took steps to address the Complainant’s legitimate concerns but failed to follow up to ensure the contractor employees had been vetted properly during the contract period.

320. When the Complainant told Subject 3 about his security concerns, Subject 3 responded that the DCO Admin had authorized the contractor employees to continue working pending the contract modification. However, we found no evidence to show that the DCO Admin confirmed the background investigations were initiated or completed to allow the contractor employees continued access.

321. Subject 3 also suggested a meeting with the Complainant’s leadership to address the Complainant’s concerns. The Complainant declined to meet with the WRNMMC ITD Chief and other ITD personnel to work out a solution to ensure the proper vetting of contractor employees despite the DCO Admin’s and Subject 2’s authorization to do so, and no one forced such a meeting to take place. Indeed, it appears they took no further action to get the PSO to move forward with initiating the BI process.

322. We concluded mistakes compounded mistakes. The investigation established WRNMMC's initial collective failure to ensure appropriate BIs for contractor employees prior to allowing them access to sensitive IT systems violated DoD 5200.2-R. We determined that WRNMMC management officials eventually took appropriate action regarding the security concerns the Complainant raised about contractors who had been granted access to WRNMMC IT systems to mitigate the identified security concerns and prevent future occurrences. However, WRNMMC acted on the wrong authority to allow exceptional contractor access and failed to document the actions taken.

323. While it may have been reasonable and prudent under the circumstances to authorize the contractor employees' access while their security checks were conducted, in fact, the minimal security checks should have been underway. WRNMMC management officials had a duty to press for resolution. The improper contractor access to the WRNMMC IT network was ultimately remedied in November 2013 in the subsequent IT support contract with STS. WRNMMC took corrective action to prevent future occurrences of the violations reported by the Complainant.

**Conclusion**

324. The allegation is **substantiated**.

**Recommendations**

325. As previously set out in allegation III, WRNMMC leadership, IT, Contracting, Human Resources, and the Personnel Security Office must work individually and in collaboration to improve proper oversight of contractor security.

**Actions Planned or Taken**

326. The WRNMMC will follow DoD 5200.2-R regarding access to IT-I and IT-II sensitive information.

327. During his first two weeks in the position, the Director, WRNMMC, sent a memorandum dated 23 October 2013 to the Secretary of Defense regarding the subject matter of this investigation. The information he received and parlayed at that time was inaccurate. Unbeknownst to the Director, members were not carrying out the security checks, minimal or otherwise and there were systematic deficiencies (confusion, misinterpreted authorities) in the security vetting. The Director's memorandum related that WRNMMC attempted to modify the security requirements in the IT contract without success. The memorandum

also indicated the previous commander apparently approved allowing the contractors to remain working, but took measures to limit permissions and work scope of the contractors. There is no written record of the previous commander's action. Upon review, it appears there was actually no need to reduce the work scope of the contractors – they were not working with classified information and were successfully providing imperative ITD services. The Director, WRNMMC was assured WRNMMC had taken remedial measures; however, he remained accountable to assure the accuracy of the information provided to the chain of command. In the future, significant decisions of this nature will be recorded.

328. DHA will replace JTF CAPMED-I 5210 with an instruction that mirrors DoD 5200.2-R. The WRNMMC PSO will ensure security clearance levels and investigation procedures are warranted by the facts and circumstances and consistent with DoD 5200.2-R. Reduce the wasteful practice of requiring contractors to have BIs and a SC when the scope of work does not demand that level of scrutiny.

329. DHA will create a records management instruction to establish records management procedures and a disposition schedule, for approval by National Archive Records Administration (NARA). NCRMD will follow the DHA records management instruction.

**Allegation Seven**

> That Subject 3, Chief Operations Officer, IT Department, WRNMMC, was receiving compensation as a Government employee while concurrently receiving compensation from SpecPro Technical Services (STS), Limited Liability Corporation, to perform work that created a conflict of interest, from 6 December 2010 to 10 September 2013, in violation of conflict of interest provisions in 5 CFR § 2635, Standards of ethical conduct for employees of the executive branch.

**Findings of Fact**

330. Complainant alleged Subject 3 worked simultaneously as a DoD GS employee and a DoD contractor employee from 6 December 2010 to 10 September 2013. Complainant stated he based this allegation on his determination that Subject 3 had both contractor employee and Government civilian Profile sheets in

JPAS; the profile sheets showed overlapping periods of employment.

331. In December 2010, STS held a Government contract that, in part, required STS to provide IT personnel at NNMC, Bethesda, Maryland. Subject 3 was employed by STS as the Manager of the One-Stop IT Help Center and his duty station was at NNMC, Bethesda, Maryland.

332. Subject 3 denied working for STS and as a Government employee concurrently. He testified that he resigned from STS on 5 December 2010, prior to accepting a Government civilian appointment. Subject 3 provided investigators with an e-mail he sent to his prior supervisors at STS, on Tuesday, 23 November 2010. The "Subject Line" of his e-mail was "2 week notice;" it advised Subject 3's STS supervisors that his last day with STS would be Sunday, 5 December 2010. Subject 3 also provided a copy of an e-mail reply he received from the President and Chief Executive Officer of STS. In the reply e-mail, The STS President acknowledged that Subject 3 was leaving STS and stated "NNMC (National Naval Medical Center) is gaining a good person."

333. An STS Senior Director confirmed that STS's records showed Subject 3 was employed by STS from 16 October 2008 to 5 December 2010.

334. Business Resource Solutions (BRS) is a human resource service company; they provided payroll services to STS in 2010. The Senior Human Resources Generalist at BRS verified that Subject 3's final paycheck from STS for the pay period ending 5 December 2010 was issued on 23 December 2010. She confirmed it was his final paycheck because it included a payout of all accrued vacation time.

335. Standard Form-50 (SF-50) is an official U.S. Office of Personnel Management (OPM) form that is used to document Federal civil service employee personnel actions and work history. Block 31 of the SF-50, known as the Service Computation Date, indicates the date the employee's Federal service began unless there is prior creditable service. We obtained a copy of Subject 3's SF-50; Block 31 shows a Service Computation Date of 6 December 2010. Subject 3 also provided copies of his Federal Tax Returns and associated W-2 Wage and Tax Statements for tax years 2011, 2012 and 2013. A review of these documents showed that Subject 3's only source of income during the period of time in question was from his Federal salary. Moreover, we found no

evidence of overlapping income from his former employer, STS, and his Federal earnings for the three years we reviewed.

336. JPAS is the DoD's official System of Record for personnel security clearance management, verification, and history. The Joint Clearance and Access Verification System (JCAVS) is a subsystem of JPAS. The Complainant provided a JCAVS Person Summary for Subject 3 to investigators as evidence that Subject 3 continued to work as a contractor employee while working as a Government civilian employee at WRNMMC. The JCAVS document we reviewed incorrectly showed that Subject 3 was separated from STS on 10 September 2013.

337. The current STS FSO also was the STS FSO during the time Subject 3 was employed by STS. The STS FSO was responsible for creating records in the JPAS for STS employees. The STS FSO testified that he was responsible for entering an inaccurate separation date in JPAS for Subject 3. The STS FSO explained that he received a telephone call from the STS NNMC site manager advising him that Subject 3 would be resigning from STS effective 5 December 2010. The STS FSO made several requests to STS personnel to provide Subject 3's exit documents, a Security Debriefing Acknowledgement and a SF-312 (Standard Form 312 – Classified Information Nondisclosure Agreement), but he did not receive the documents he requested. The STS FSO said that as time passed he simply forgot about the matter and eventually it slipped his mind altogether until 10 September 2013 when he received a system generated alert in JPAS about Subject 3.

338. The STS FSO stated that the notification he received was an indication that an incident report had been filed about Subject 3. The STS FSO said that he contacted the site manager at WRNMMC to verify Subject 3's status as a STS employee. After confirming Subject 1 was no longer an STS employee and realizing his mistake not to document Subject 3's change in employment status in JPAS several years earlier, the STS FSO made an entry in JPAS on 10 September 2013 to document Subject 3's change in employment status. The STS FSO further explained JPAS did not afford him with an option to backdate event thus creating the apparent overlap that the Complainant noted in his review of JPAS information.

**Regulations**

339. Several provisions in 5 CFR § 2635 could have applied if the facts demonstrated Subject 3 continued working for a DoD contractor after he became a DoD Government civilian employee.

Such provisions would include 5 CFR 2635.402, Disqualifying Financial Interests, 5 CFR 2635.502, Personnel and Business Relationships, and 5 CFR 2635.802, "Conflicting Outside Employment and Activities."

**Discussion and Analysis**

340. We determined that Subject 3, a former employee at STS, ended his employment with STS on 5 December 2010. We also determined that Subject 3 began his Federal civil service employment on 6 December 2010 and, moreover, at no time did he receive compensation simultaneously from STS and the Government. We based the foregoing determination on a thorough review of Subject 3's SF-50s, his Federal Tax Returns for 2011, 2012 and 2013, and other evidence documenting the period of his employment by STS.

341. We further determined that the STS FSO did not make a timely entry into JPAS about Subject 3's departure from STS. We concluded that the STS FSO's late entry into JPAS about Subject 3 on 10 September 2013 resulted in an inaccurate portrayal of Subject 3 work history in JPAS; this inaccuracy was noted by the Complainant and reasonably believed by him to be fact. It was, however, not fact but an error. Having found no credible evidence to support the allegation that Subject 3 engaged in outside employment or received compensation from STS or any other organization that would conflict with his duties as a Government employee, we concluded that he did not have a conflict of interest.

**Conclusion**

The allegation is **not substantiated**.

**Recommendations**

342. Correct the JPAS record of Subject 3.

**Actions Planned or Taken**

343. The WRNMMC IG office advised the STS FSO, via e-mail on 25 August 2014, that he could take action to correct the inaccurate information in JPAS related to Subject 3's "Separation Date" to ensure the fidelity of the JPAS. The WRNMMC IG office informed the STS FSO that an individual in the JPAS Program Management Support Office stated the "separation date" data filed in JPAS could be backdated without fear of data loss.

344. On 10 September 2014, the STS FSO confirmed that the correct “Separation Date” for Subject 3 had been submitted in the JPAS.

This page intentionally blank to facilitate two sided printing

## Appendix A – Reference Documents

1. TASKORD R101210.01, Subject: BRAC TRANSITION NAVY IT ACCESS 071200R dated 7 DEC 2010

2. SubK Emp1 ID Card and Vehicle Pass Application and Memorandum dated 4 December 2012

3. Appointment Letter from National Naval Medical Center to Complainant appointing him as the National Naval Medical Center's Management Analyst for Command Personnel Security/Adjudication dated 18 October 18 2010

4. E-mails between Complainant and a naval officer Subject: Contractor Security Clearance Process dated 30 May 30 2013

5. E-mail from Complainant to WRNMMC COS, Subject: National Security Concerns dated 31 May 2013

6. Complainant’s NCIS Certificate of Training for Naval Security Manager Course dated 20-23 June 2011

7. E-mail from Subject 2 to Complainant, Subject: Complainant’s PD, dated June 3, 2013

8. E-mails between Subject 2 and Complainant, Subject: Complainant’s PSO Coworker dated 10 June 2013

9. E-mails between Complainant, Subject 1, Subject 2 the WRNMMC IASA, Kor Emp 1, and the WRNMMC CIO/COR, Subject: CAC Request ICO Kor Emp 2 dated 16 August – 9 September 2013

10. E-mails between Complainant and Subject 1 dated 9-17 September 2013, Subject: Kor Emp 1 (National Security Concern)

11. Incident Report on Subject 3 dated 10 September 2013

12. JCAVS Report on Subject 3 dated 12 September 2013

13. Incident Report on Subject 2, USN, dated 3 October 2013

14. Memorandum from Complainant to Subject 2, USN, regarding an informal grievance dated 4 October 2013

15. E-mail from Complainant to WRNMMC Chief of Human Resources and WRNMMC Director of Executive Services (No subject) dated 21 November 2013

16. E-Clearance document on Kor Emp 1 dated 30 August 2013)

17. E-mails between Subject 2, the WRNMMC ITD Chief, Complainant, and the WRNMMC CIO/COR, Subject: WRNMMC is not processing our NACLCs dated 7 December 2012

18. E-mails between Subject 3, the WRNMMC ITD Chief, and Complainant, Subject: Meeting with the WRNMMC ITD Chief dated December 7-11, 2013

19. E-mails between Subject 2, USN, the WRNMMC ITD Chief, and Complainant, Subject: Security Clearance for Contractor, dated January 10-11, 2013

20. E-mail from Complainant to the WRNMMC ITD Chief, Subject: Security Clearance for Contractor dated 14 January 2013

21. Contract W91YTZ-12-C-0157 (MedPro) for period 28 September 2012 to 27 September 2013

22. E-mail from an NDW representative to CNIC Investigator confirming Kor Emp 1 was not issued a RAPIDGate ID card, dated 19 June 2014

23. Data Request System (DRS) Data on Kor Emp 1's CAC status

24. Memo regarding Implementation of Military Health System Governance Reform dated 11 March 2013

25. Tasker Package OSD011554-13 regarding September 2013 complaint to SECDEF

26. STS Contract: N00189-14-C-Z004 for period 1 November 2013 to 31 July 2014

27. STS Contract N00189-11-D-Z027 Task Order Number 00B1 for 1 October 2012 to 28 February 2013

28. STS Contract N00189-11-Z043 for period 1 August 2014 to 31 December 2014

29. STS Contract N00189-14-C-Z004, modifications 1,2,3,& 4

30. Memo from Current CO, NSAB to Commandant, NDW, regarding WRNMMC and NSAB Security Concerns, dated 2 October 2013

31. Clearance Status Sheet provided by the WRNMMC ITD Chief dated 3 July 2014

32. E-mail from the NSAB DSO to the NSAB ED regarding whether Complainant responded to request for information dated 18 September 2013

33. List of contractor employees on Medpro/B.E.A.T. contract provided by the WRNMMC CIO/COR dated 23 July 2014

34. Subject 2, USN, (Evaluations) for period 29 September 2011 to 28 April 2014

35. Defense Personnel System (DPS) Printouts on Contractors

36. Complainant's Position Description

37. Complainant’s PSO Coworker Position Description

38. Personnel Change of Status for Subject 3

39. E-mail from STS FSO regarding Subject 3 separation

40. SF 50 (Effective Date 1-12-14) for Subject 3

41. NSAB Security Organization Chart dated 27 March 2012

42. WRNMMC Chief of Human Resources Command Security Manager designation letter dated 23 October 2013

43. List of MedPro contractor employees provided by the MedPro General Manager

44. E-mail from NSAB DSO to IOs regarding the WRNMMC badge dated 7 August 2014

45. E-mail from Subject 1’s immediate supervisor to IOs regarding the Navy’s CLEOC dated 7 August 2014

46. US DoD IG Report 2013-134, “Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks,” dated 16 September 2013

47. E-mails from Subject 1 to IOs regarding DoD IG Report 2013-134, points of contact for the report, and the NCIC check on Kor Emp 1, dated 6-7 August 2014

48. E-mail from Subject 1 to IOs regarding NCIC check on Kor Emp 1 dated 6 August 2014

49. CNICINST 5530.14 “Projected Upcoming Changes to CNICINST 5530.14,” dated 7 July 2011

50. E-mail from Subject 1 to IOs regarding standard operating procedures for issuing badges to contractors, dated 5 August 2014

51. E-mail from Subject 1 to IOs regarding NACI check on Kor Emp 1, dated 4 August 2014

52. E-mail from Subject 1 to IOs regarding 21 e-mails he had on the situation about Kor Emp 1's access to NSAB, dated 21 July 2014

53. E-mail from Subject 1 to IOs regarding issuing badges at NSAB, including an attachment of NNMCINST 5530.1C Chapter 5 (Access), "Physical Security Manual for Naval Medical Center (NNMC)," dated 10 November 2009, e-mailed to IOs on 21 July 2014

54. E-mails between Subject 1 and Complainant regarding Kor Emp 1, dated 9 & 11 September 2013

55. E-mails between NSAB DSO, Subject 1, and Complainant regarding Kor Emp 1, dated 9, 11, 13, & 17 September 2013

56. E-mails between Complainant and Subject 1 regarding Kor Emp 1, dated 11 September 2013

57. E-mails between Complainant and Subject 1 regarding revoking Kor Emp 1's access, dated 11 September 2013

58. E-mails between Complainant and Subject 1 regarding Kor Emp 1, dated 9 September 2013

59. E-mails between the IOs and the NSAB DSO regarding access control at NSAB, dated 24 June 2014, 1 July 2014, 7 July 2014, 15 July 2014

60. E-mails between IOs and the NSAB DSO regarding access control at NSAB, dated 15 & 16 July 2014

61. E-mails between IOs with DMDC Reporting System information regarding Kor Emp 1's CAC, dated 1 August 2014

62. E-mails between Complainant, the NSAB DSO, and the NSAB ED regarding concerns about Kor Emp 1, dated 17 & 18 September 2014

63. E-mails between IOs and an NDW representative regarding Kor Emp 1 and RAPIDGate ID card, dated 17 & 19 June 2014

64. E-mail from STS Senior Director to IOs regarding Subject 3's employment with STS, dated 27 July 2014

65. JCAVS Person Summary on Subject 3, dated 10 & 12 September 2013

66. E-mails between STS FSO and IOs regarding Subject 3's employment, dated 30 July 2014

67. E-mail from Subject 3, regarding 2 week notice to SpecPro, Inc., dated 30 July 2014

68. E-mail from Subject 3 regarding discussion with SpecPro's President, dated 30 July 2014

69. Personnel Change of Status for Subject 3, Employee Separation Notice from SpecPro, Inc., dated 6 December 2010

70. SF-50 for Subject 3, dated 12 January 2014

71. US Individual Income Tax Return 2011 for Subject 3, including W-2 for 2011

72. SF-50 for Subject 3, dated 6 December 2010

73. US Individual Income Tax Return 2012 for Subject 3, including W-2 for 2012

74. GS-Schedule Salary Table for Washington, DC for 2012, effective 1 January 2012

75. US Individual Income Tax Return 2013 for Subject 3, including W-2 for 2013

76. SF-50 for Subject 3, dated 18 December 2011

77. SF-50 for Subject 3, dated 17 November 2013

78. E-mail from IOs to the Chief of the WRNMMC Staffing and Classification Branch in the NCRMD Civilian Human Resources Center requesting Subject 3's SF-50's for the period of 6 December 2010 through 1 January 2014, dated 7 August 2014

79. E-mail from IOs to STS FSO regarding JPAS Data Input, dated 30 July 2014

80. E-mails between IOs and Subject 1 regarding proposed changes to CNICINST, dated 9 & 11 April 2014

81. E-mails between IOs and Subject 1 regarding RAPIDGate, NCACS, NCIC checks concerning Kor Emp 1, dated 9 & 11 August 2014

82. Joint Task Force (JTF) CAPMED-I, 5210.01, Personnel Security Program (PSP), dated 13 December 2011

83. JTF CAPMED-I 5210.01 revised, dated 22 April 2013

84. Memorandum from Subject 2 to Health Services Contractor and Contracting Entities, “Employment Contract Clause for Accessing Sensitive/Classified, and/or Access to Sensitive IT Data and Information, dated 2 February 2012

85. E-mail from the B.E.A.T Vice President to the WRNMMC CIO/COR and Subject 3 regarding NACLC checks, dated 7 December 2012

86. Executive Order 12968 Section 1.2.(c)

87. Executive Order 10450 Section 3(c)

88. 5 United States Code Section 552 (a) (e) (10)

89. 5 Code of Federal Regulations Section 2635.802 “Conflicting Outside Employment and Activities.”

90. OSC Tasking Letter dated 11 February 2014

91. Memorandum from Director, WRNMMC dated 23 October 2013

92. DoD Instruction 5200.2R, DOD Personnel Security Program

93. SECNAV Instruction 5510.30

94. NSAB’s Standard Operation Procedures (SOPs) for Access Control

95. CNIC 5530.14, “Projected/Upcoming Changes to CNIC 5530.14 Ashore Protection Program”, dated 7 July 2011

96. CNIC 5530.14A “Ashore Protection Program,” May 2013

97. CNIC Note 5530, Enclosure 1

98. Complainant’s letter to the Secretary of Defense dated 23 September 2013

99. DTM-09-012 “Interim Policy Guidance for DoD Physical Access Control”

100. OPNAVINST 5530.14E, “Navy Physical Security and Law Enforcement Program,” dated 19 April 2010

101. Joint Commission Requirement, dated 13 January 2009

102. E-mail message from WRNMMC IG to WRNMMC/DHA attorneys and WRNMMC IG Investigator Subject, Navy General Counsel Questions/Concerns regarding OSC 0535 Draft Report for External Review 1330, dated 18 August 2014

103. E-mail message from Counsel, NAVINSGEN to CNIC Supervisory Investigator, CNIC Investigator, and another NAVINSGEN attorney, Subject: Please call me at your earliest convenience to discuss the way ahead, dated 17 August 2014

104. E-mail message from Subject 1 to the IOS regarding results of the 2014 Audit at NSAB, dated 27 August 2014

105. DHA & NCR MD Organizational Chart

106. OPNAV Notice 5400 Rename Change for Walter Reed dated 12 February 2014

107. Kor Emp 2 Check-In Sheet

108. MedPro Contract P00001, P00002, & P00003

109. E-mail message between Subject 2 and the Complainant about his position description, dated 3 June 2013

110. Report No. DODIG-2013-134, Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks, dated 16 September 2013

111. E-mail message between IOs and Kor Emp 1 in which Kor Emp 1 declined to participate in the investigation, dated 29 July 2014

112. NSABETHINST 5530.2, “Access Control Procedures,” 15 December 2011

113. Executive Order 10450, Section 3(a)

114. 5 CFR 2635, Standards of Ethical Conduct for Employees of the Executive Branch

115. DD 5500.19, Cooperating with the United States Office of Special Counsel (OSC)

116. 5 USC 1213

117. NNATNAVMEDCENINST 5527.1, Criminal Background Investigation Standards and Requirements for Contractual Employment on board National Naval Medical Center

118. NATNAVMEDCENINST 5530.1C, Physical Security Manual for National Naval Medical Center

119. OPNAVINST 1752.3

120. E-mail messages from Subject 1 regarding 2014 audit at NSAB, dated 25 & 27 August 2014

121. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 8 July 2014

122. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 24 July 2014

123. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 30 July 2014

124. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 1 August 2014

125. E-mails from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 7 August 2014

126. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 11 August 2014

127. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 12 August 2014

128. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 15 August 2014

129. E-mail from Complainant to CNIC Investigator, Subject: RE: IG Case 201401284, dated 26 August 2014

130. E-mail from Complainant to Subject 2, the WRNMMC Human Resources Assistance Department Chief, the WRNMMC Division Oficer for Manpower, and Complainant’s PSO Coworker, dated 10 February 2012

131. E-mail from the B.E.A.T. Presidnet to CNIC Investigator, Subject: RE: IG Case 201401284, dated 22 August 2014

132. E-mails from WRNMMC Chief of Human Resources to CNIC Investigator, Subject: RE: List of Contractors (3), dated 27 August 2014

133. E-mail from SpecPro WRNMMC site manager to CNIC Investigator, Subject: RE: Request for assistance in an Official Investigation, dated 12 August 2014

134. E-mail from CNIC Security Specialist to CNIC Investigator, Subject: RE: Contractors, dated 20 August 2014

135. Spreadsheet from CNIC personnel security office, containing MedPro and BEAT contractors, along with security clearance/background investigation information, obtained 20 August 2014

136. E-mail from CNIC Security Specialist to CNIC Investigator, Subject: RE: JPAS Search, dated 22 August 2014

137. Spreadsheet from CNIC personnel security office, containing MedPro and BEAT contractors, along with security clearance/background investigation information, obtained 22 August 2014

138. E-mail from CNIC Security Investigator to CNIC Investigator, Subject: RE: STS Contractors, dated 25 August 2014

139. Spreadsheet from CNIC personnel security office, containing STS contractors, along with security clearance/background investigation information, obtained 25 August 2014

140. E-mail from WRNMMC IG Investigator to CNIC Investigator & NAVINSGEN Investigator, Subject: Follow up contact request, dated 28 July 2014

141. E-mail from WRNMMC IG Investigator to CNIC Investigator & NAVINSGEN Investigator, Subject: RE: List of contractors, dated 29 July 2014

142. MedPro/BEAT employee spreadsheet, containing information from the current WRNMMC Security Manager, dated 29 July 2014

143. E-mails from Subject 3 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 12 August 2014

144. E-mails from Subject 3 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 14 August 2014

145. E-mails from Subject 3 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 25 August 2014

146. E-mail from Subject 3 to CNIC Investigator, Subject: RE: CAC Request ICO Kor Emp 2, dated 27 August 2014

147. E-mail from MedPro General Manager to NAVINSGEN Investigator, Subject: RE: Request for assistance in an Official Investigation, dated 8 August 2014

148. MedPro Employee listing provided by MedPro, dated 8 August 2014

149. E-mail from MedPro General Manager to CNIC Investigator, Subject: RE: Request for assistance in an Official Investigation, dated 21 August 2014

150. MedPro Employee listing provided by MedPro, dated 21 August 2014

151. E-mail from Subject 2 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 8 August 2014

152. E-mails from Subject 2 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 11 August 2014

153. E-mail from Subject 2 to CNIC Investigator, Subject: RE: IG Case 201401284, dated 25 August 2014

154. E-mail from the WRNMMC ITD Chief to CNIC Investigator, Subject: RE: IG Case 201401284, dated 4 August 2014

155. E-mail from the WRNMMC ITD Chief to CNIC Investigator, Subject: RE: IG Case 201401284, dated 7 August 2014

156. E-mails from the WRNMMC ITD Chief to CNIC Investigator, Subject: RE: IG Case 201401284, dated 12 August 2014

157. E-mail from the WRNMMC ITD Chief to CNIC Investigator, Subject: RE: IG Case 201401284, dated 22 August 2014

158. E-mails between Complainant, Subject 2, and Subject 1, Subject: RE: CAC Request ICO Kor Emp 2, dated 9 September 2013

159. WRNMMC Contractor Packet 2014, includes Check-in Sheet, Revised June 2014

160. Memorandum for the Record provided by the former DCO-Admin, dated 23 January 2013

161. WRNMMC IT Department Organizational Chart, August 2014

162. Department of the Navy Local Population ID Card/Base Access Pass Registration, SECNAV 5512/1, April 2014

163. Chart of STS contract clearance status, as of 15 August 2014.

164. Memorandum for File, WRNMMC Director of Administration – 9 July 2014

165. Memorandum for File, Subject 3 interview – 9 September 2014

166. Memorandum for File, WRNMMC ITD Chief interview – 11 July 2014

167. Memorandum for File, WRNMMC ITD Chief interview – 25 August 2014

This page intentionally blank to facilitate two sided printing

## Appendix B – Witness List

1. Complainant and his attorney, by telephone

2. Director of Administration, WRNMMC, by telephone (not mentioned by name in report)

3. Current CO, NSAB, in person

4. Directive of Executive Services, DHA NCR MEDDIR, in person (not mentioned by name in report)

5. Supervisory Statistician & Chief, Personnel Security, Office of the Under Secretary of Defense for Intelligence, Office of the Secretary of Defense, by e-mail (not mentioned by name in report)

6. Chief of Human Resources, WRNMMC, in person (not mentioned by name in report)

7. HR Manpower Analyst, WRNMMC, in person (not mentioned by name in report)

8. Former Deputy Commander for Administration, (DCO-Admin) WRNMMC, by telephone

9. Facility Security Officer, SpecPro Technical Services (STS FSO), by telephone

10. Former Assistant Director for Administration, WRNMMC, by telephone (not mentioned by name in report)

11. CIO/COR, IT Department, WRNMMC (WRNMMC CIO/COR), in person

12. Installation Security Officer and Director, Security Operations, NSAB NSAB DSO), by telephone

13. Former CO NSAB, by telephone

14. B.E.A.T. Subcontractor employee (Kor Emp 2), in person (note: STS contractor employee #1 (Kor Emp 1), refused to be interviewed)

15. Information Assurance Systems Administrator, WRNMMC (WRNMMC IASA), in person

16. Subject 3, COO, WRNMMC, in person

17. Executive Director, NSAB (NSAB ED), by telephone

18. Second former Assistant Director for Administration, WRNMMC, by telephone (not mentioned by name in report)

19. Contract Program Manager for AAI, in-person (not mentioned by name in report)

20. Current Security Manager, WRNMMC, by telephone

21. Receptionist, STS IT contractor , WRNMMC, by telephone (not mentioned by name in report)

22. Trusted Agent Security Manager and PSS, HR, WRNMMC, in person (not mentioned by name in report)

23. Subject 2, USN, Former Chief, Human Resources and Manpower, WRNMMC, by telephone and later in person

24. Subject 1, Security Specialist, NSAB, in person

25. Chief of the Logistics Department, WRNMMC, by telephone

26. CNIC Deputy Director of Operations, in person

27. Supervisory Safety and Occupational Health Specialist, NDW, by telephone (not mentioned by name in report)

28. WRNMMC CIO and Chief, IT Department, WRNMMC (WRNMMC ITD Chief), in person

29. Chief Technology Officer, IT Department, WRNMMC (WRNMMC IT CTO), in person

30. B.E.A.T Vice President and Program Manager, by telephone

31. Senior Human Resources Generalist, Business Resource Solutions, by telephone

## Appendix C – Consolidated List of Recommendations

Allegation One Recommendations

1. That NSAB revise NSABETHINST 5530.2 to incorporate the requirements set forth in CNICINST 5530.14 and DTM 09-012. Specifically, the installation access control standards should include requirements for conducting NCIC index, Sex Offender Registry, Terrorist Screening Database, and debarment checks to determine the fitness of an individual requesting and/or requiring access credentials.

2. As currently written, the NSABETHINST 5530.2 4d(4)(e) allows conflicting interpretations with regards to issuing WRNMMC badges to contractors. Recommend NSAB clarify the requirement in this paragraph.

3. That CNIC ensure that lessons learned from this event are widely distributed with action directed to all Navy Regions Commanders to review procedures at all subordinate Naval Support Activities under their command.

Allegation Two Recommendations

4. That NSABETHINST 5530.2 be rewritten to incorporate the requirements set forth in CNICINST 5530.14. Specifically, the installation access control standards should include requirements for conducting NCIC, Sex Offender Registry, and debarment checks to determine the fitness of an individual requesting and/or requiring unescorted access credentials. As currently written, the instruction allows conflicting interpretations with regards to the issuing of contractor badges.

5. That CNIC direct all Navy Regions to screen all current contractor employees to ensure that they were submitted for a NCIC, Sex Offender Registry, and debarment check before they were issued their current installation access credential and anyone found to have not undergone these checks be immediately submitted for such checks. Anyone found not in compliance with access requirements set forth in CNICINST 5530.14 shall thereafter have their installation access revoked.

6. That CNIC ensure that lessons learned from this event are widely distributed with action directed to all Navy Region

Commanders to review procedures at all Naval Support Activities under their command.

Allegation Three Recommendations

7. That WRNMMC ensure ITD contractor employees have the appropriate BI/SC prior to initiating work on subsequent IT contracts. If contractors are found to be non-compliant, recommend WRNMMC officials reduce contractors' duties or remove them from the contract until they have the appropriate BI/SC.

8. Specifically, regarding the three individuals currently working on the STS contract without a clearance, we recommended WRNMMC officials remove the contractors from the contract pending completion of their clearance.

9. WRNMMC ITD should work with human resources and the contracting officer to determine whether ITD personnel need IT-I or IT-II sensitive information access and comply with the security requirements of DoD 5200.2-R. When determined necessary for IT-I access, contractors must have a BI and an approved SC. WRNMMC ITD should determine whether specific contractor employees will have access to classified information or critical-sensitive information, and when they will not. The contract will clearly define contractor employee security requirements and require the contractor to bear the cost of BIs. When a SC is required, the contract should hold the contractor responsible to hire and provide only personnel with a previously approved Secret clearance or bear the costs of obtaining a SC with a NACLC.

10. WRNMMC and NSAB should suspend base access and information systems privileges of all contractor employees who are determined to be working without interim or permanent security checks. The contracting officer will work with the contractor and NSAB to resolve the deficiency. If contractor employees are found to be non-compliant, recommend WRNMMC officials remove the contractor employees from the contract pending completion of their clearance or have their work duties reduced in scope until their clearance is granted pending compliance with security check procedures.

11. All WRNMMC contract personnel should undergo a National Agency Check with Law Enforcement and Credit (NACLC).

## Allegation Four Recommendations

12. That WRNMMC ensure that ITD contractors have the appropriate BI/SC prior to being granted access to IT systems. If contractors are found to be non-compliant, recommend WRNMMC officials remove them from the contract until they have the appropriate BI/SC.

13. WRNMMC HR should coordinate with the WRNMMC PSO and NSAB to expedite security checks of all contractor personnel, report on progress of onboarding contractors, and employees, and serve notice of serious criminal violations, etc.

14. Allegation Five Recommendations

15. There are no recommendations for this allegation, which was not substantiated.

## Allegation Six Recommendations

16. As previously set out in allegation III, WRNMMC leadership, IT, Contracting, Human Resources, and the Personnel Security Office must work individually and in collaboration to improve proper oversight of contractor security.

## Allegation Seven Recommendations

17. That the inaccurate entries in JPAS for Subject 1 be corrected.

This page intentionally blank to preserve section numbering.
Delete from PDF version of the report.