DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

JUL 10 2013

The Honorable Carolyn N. Lerner
Special Counsel
U.S. Office of Special Counsel
1730 M. Street, N.W. Suite 300
Washington, DC 20036-4505
Attn: Catherine A. McMullen, Chief Disclosure Unit

Re: OSC File No. DI-13-0923

Dear Ms. Lerner:

This is in response to your April 2, 2013 letter to Secretary Hagel pertaining to OSC File No. DI-13-0923. I have been delegated the authority to review and sign this report pursuant to 5 U.S.C. § 1213(d)(5) and Department of Defense (DoD) Directive 5500.19 as the designated Senior Management Official for the Office of the Secretary of Defense (OSD) which has cognizance over the affected field activity, Washington Headquarters Services.

Enclosed is the report of investigation in response to allegations by a whistleblower that employees of Washington Headquarters Services (WHS), Facilities Services Directorate (FSD) failed to follow procedures to safeguard personally identifiable information (PII) and failed to contact the appropriate individuals once a sensitive PII breach had occurred.

I have reviewed the report and concur with the findings and recommendations of the investigating officer. Because of the low risk of harm, I have determined that notification of affected employees is not warranted. Of note, no allegations of whistleblower reprisal were raised – nor were any discovered during the investigation.

As detailed in the report, the underlying breach of PII appears to have been caused by the consolidation of legacy WHS Information Technology Management Division (ITMD) data into the OSD CIO (EITSD) technology infrastructure which resulted in security gaps in folder and shared drive access by authenticated users. Efforts to safeguard PII on the information network are on-going and will continue until fully resolved. The Director FSD and the Director, Enterprise Information Technology Services will ensure PII is properly safeguarded and accessed only by authorized personnel for an official government purpose.

The PII of 461 WHS employees was available and accessible to other WHS employees who did not have an official "need to know"; however, I have determined the risk of harm to the individuals is "Low" and does not warrant notification. I make this determination following consultation with the DoD Privacy and Civil Liberties Office. A key factor in my decision is the fact that the PII was only accessible to persons with access to the EITSD Enterprise, each of whom has been screened through various background checks in order to gain access to the network.

Although the investigation revealed that the individuals affected by the breach were not notified, the low risk presented did not outweigh the other risks associated with overzealous notification. As outlined in Director, Administration & Management Memorandum "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations," August 2, 2012, "Notification when there is little or no risk of harm might create unnecessary concern and confusion. Overzealous notifications resulting from notification criteria which are too strict could render all such notifications less effective because consumers could become numb to them and fail to act when risks are truly significant."

In addition to the remedial measures detailed in the report, I have directed the publication of a new Operating Instruction that assigns responsibilities and identifies procedures for immediate reporting of a breach, immediate response, and conducting of a risk assessment. These collective measures will ensure a more timely and transparent response in the event of future breaches.

Finally, although no allegations of whistleblower reprisal were raised or discovered during the investigation, I have directed senior WHS leadership to reiterate to their employees the protections afforded whistleblowers under DoD policy. Retaliation is unlawful and will not be tolerated.

If you have any questions regarding this matter, please contact me or Mr. John Albanese, General Counsel for WHS at, 703-693-7374.

Sincerely,

William E. Brazis
Director

Enclosure:
As stated

cc:
Secretary of Defense

ENCLOSURE 1

REPORT OF INVESTIGATION RE: OSC DI-13-0932

1. SUMMARY OF THE INFORMATION WITH RESPECT TO WHICH THE INVESTIGATION WAS INITIATED

In a letter dated April 2, 2013, from the U.S. Office of Special Counsel (OSC) to the Secretary of Defense, The Special Counsel directed that an investigation be conducted concerning a whistleblower's allegations that Washington Headquarters Services (WHS) Facilities Services Directorate (FSD) failed to follow appropriate procedures for safeguarding sensitive personally identifiable information (PII) and failed to contact the appropriate individuals once a sensitive PII breach occurred, thus placing employees and other members of the public at risk. Issues raised were:

- The whistleblower discovered numerous instances where documents containing sensitive PI, such as Social Security numbers, were stored on the WHS FSD shared computer drive in violation of DoD policy; and

- The individuals whose sensitive PII was improperly stored on the shared drive were not properly notified pursuant to DoD policy.

The whistleblower disclosed that nine (9) times between October 2012 and February 2013, he or she discovered numerous documents containing sensitive PII improperly stored on the WHS FSD shared network drive (S: drive). On those occasions, the whistleblower found over 100 pages of sensitive information belonging to DoD employees.

October 19, 2012: The whistleblower first discovered records containing sensitive PII on the S: drive and immediately notified Mr. Anthony Conques[4] and his supervisor, Mr. Paul McMahon[5] along with the Directorate Security Officers.

November 27, 2012: The whistleblower again notified management that records containing sensitive PII were still on the S: drive. Management told the whistleblower that they were working to address the problem.

January 16, 2013: The whistleblower noticed that management removed some of the records containing sensitive PII from the S: drive, however, records containing sensitive PII were still available. Even though management was taking steps to remove the records containing PII permanently, it does not appear that management attempted to limit access to the S: drive during that process.

March 26, 2013: Records containing PII were still available on the S: drive.

---

[4] Mr. Conques was not interviewed as he retired in December 2012 and, there is no indication he possessed information that would have changed the results of this investigation.

[5] Mr. McMahon, Assistant Director of Operations, FSD, was interviewed May 1, 2013. He was aware of the issue and coordinated with Mr. David Butler, Director, FSD Directorate Management Division (labor and employee relations; management support), who in turn monitored the issue. Neither Mr. McMahon nor Mr. Butler had any record that would have contributed to the summary of evidence in Section 4.

According to the whistleblower, WHS management failed to follow DoD policy regarding notification of the individuals whose sensitive PII may have been lost, stolen or compromised. The whistleblower found records containing his or her PII on the S: drive, but was not notified of the sensitive PII breach pursuant to DoD policies.

2. POLICIES REFERRED TO BY THE OSC

a. Privacy Act of 1974, see 5 U.S.C 522a (e)(10):

(a) Agencies are responsible for establishing appropriate safeguards to protect privacy information.

b. DoD Privacy Program 5400.11-R (May 14, 2007):

(a) DoD components shall establish appropriate safeguards to ensure that the records are protected from unauthorized access, alteration or disclosure and that their confidentiality is preserved and protected (C1.4.1. of DoD 5400.11-R).

(b) A PII breach occurs when there is an "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected (CL1.10.)

(b1) If records containing personal information are lost, stolen, or compromised, the DoD component must promptly notify the individual of any loss, theft or compromise.

(b2) When a breach occurs, the component must notify the individuals as soon as possible, but not later than ten (10) working days after the loss, theft, or compromise is discovered and the identifies of the individuals are ascertained.

(b3) The component may delay notifying the affected individuals if there is good cause, but the delay shall only be for a reasonable amount of time. To determine what constitutes a reasonable amount of time, the potential harm to the affected individual must be weight against the necessity for delayed notification.

(b4) Notice to the affected individual must include the specific data involved in the breach, and the individual must be informed if his or her name, Social Security number, and date of birth have potentially been compromised.

(b5) The individual must be informed of what protective actions the component is taking or the individual can take to mitigate potential future harm.

3. DESCRIPTION OF THE CONDUCT OF THE INVESTIGATION

On April 8, 2013, the OSC letter was received by Washington Headquarters Services (WHS) correspondence control personnel and entered into the Staff Action Control & Coordination Program (SACCP) system.

On April 9, 2013, the Acting Deputy Director, WHS, Mr. Sajeel Ahmed, directed personnel from FSD and Enterprise Information System Technology Directorate (EITSD), WHS, to immediately start scanning the FSD shared drives to identify PII, so that an assessment could be conducted to either remove the PII or to make sure the PII was under proper access controls. Mr. James Teller, EITSD, initiated action to begin searching FSD Leased Facilities Directorate (LFD) share drive for PII.

On April 25, 2013, Mr. Ahmed, appointed Mr. Thomas Prudhomme, Component Security Manager, WHS, as the Investigating Officer.

a. Allegation 1:

The whistleblower discovered numerous instances where documents containing sensitive PII, such as Social Security numbers, were stored on the WHS shared computer drive in violation of DoD policy.

IO Findings: Allegation Substantiated

Access to PII by unauthorized WHS personnel likely occurred because the EITSD Windows XP to Windows 7 migration provided the file path to each mapped drive that allowed FSD users to determine the relationship between directory/file paths and search for information, which possibly contained unsecured folders and PII files previously hidden from view.
The access initially occurred in October 2012 and was reported by Mr. Dennis Luquette, Contracting Officer, WHS Acquisition Directorate (AD). Mr. Luquette reported seeing a file containing PII of FSD individuals. From this point, several members of SPMD were able to access PII on the shared drive that should have been restricted from their view.

Discussion

On October 19, 2012, Mr. Dennis Luquette, AD, reported to Mr. Dave Mayberry, Chief Space Management Branch, FSD SPMD, that he (Luquette) discovered an FSD document containing PII on the shared drive that should not have been available to him. Mr. Mayberry asked Ms. Tina Brown-Richards, Security Monitor, FSD SPMD if she could fix the situation.

In an effort to determine the magnitude of the incident, Ms. Brown-Richards conducted random checks of the shared drive, finding many files containing PII that should not have been available to her. Between October 19, 2012 and February 11, 2013, several communications took place between SPMD management, Ms. Brown-Richards, Mr. Ron House and Mr. Louis Vazquez, FSD Security, to report files containing PII which were subsequently reported to Mr. Ken Ballard, Customer Resource Manager, EITSD, requesting that he assist with removing the files from the shared drive.

On April 29, 2013, the investigating officer met with Ms. Brown-Richards and, while using Ms. Brown-Richards' computer, they were able to access AD folders containing PII. Ms. Brown-Richards should not have had access to the AD folders. This effort was to recreate the unauthorized access. No PII was copied or printed.

Additionally, Ms. Brown-Richards provided as a sample of PII found, printed documents found during her review of the shared drive that she had previously reported to FSD management. These five (5) documents (combined) contained the following PII:

a. 461 individuals. This includes one (1) individual each from Pentagon Force Protection Agency and Acquisition Directorate, and 459 individuals from FSD (and includes the PII of Ms. Brown-Richards).

b. PII included: SSN (for all individuals); date and place of birth; personal email address, home phone number and home address; salary; and supervisor's cash award amount.

Remedial Actions Taken

Mr. Tony Smith, Network Operations Problem Management Team Lead, EITSD, with the assistance of Mr. Joe Wojtyna, Investigative Search Request Specialist, EITSD, are continuing efforts to search for files containing PII on the shared drive, and moving those files to a "quarantine" folder that only the investigating officer and SPMD "Trusted Agents" will be able to access. The process consists of searching the shared drive for PII key words (e.g. social security number; DOB) or for specific numeric sequences (e.g. "???-??-????") indicating the actual digits of a social security number.

Mr. Tony Smith was unable to locate documentation to show a response by EITSD personnel and action taken. However, based on the email communications described under Section 4 of this report, EITSD personnel did stay in communication with FSD personnel from the initial complaint in October 2012.

The SPMD "Trusted Agents" (Mr. Dave Mayberry, Mr. Bill Nicholson, Mr. John Dupont and Mr. Chuck Boyd) are higher-level supervisors with SPMD and are responsible to review the files in "quarantine" for PII and determine appropriate disposition of each file. As higher-level supervisors tasked to review files containing PII, the "Trusted Agents" are engaged in the scope of their employment and are required to protect and maintain confidentiality of the material they review.

To date, EITSD personnel have responded to the complaints of PII on the shared drive and have implemented the following actions to limit access to PII and to mitigate the risk of future inadvertent PII disclosures.

a. May 2, 2013, the EITSD Network Operations Branch Chief, in coordination with the EITSD Operations Director, appointed Mr. Tony Smith as the EITSD Operations representative to the WHS investigating officer, Mr. Thomas Prudhomme.

b. May 4, 2013, Mr. Smith determined the consolidation of legacy WHS Information Technology Management Division (ITMD)[6] data into the OSD CIO (EITSD) technology infrastructure, introduced security gaps in folder and shared drive access by authenticated users. The legacy WHS ITMD practice of granting network share/folder access by user in lieu of using Windows security groups is not consistent with best business practice. EITSD Operations will migrate all WHS Directorates to new common IT and security infrastructure to minimize future PII breaches.

c. EITSD Operations is implementing the following actions:

    a. Restrict SPMD user permissions to SPMD folders on the WHS domain – completed

    b. Conduct investigative search for PII within SPMD network share.

    c. Quarantine PII found in a restricted folder granting access to the SPMD Trusted Agents.

    d. Create SPMD new share on the new OSD domain, establish correct permissions and drive mappings.

b. Allegation 2:

The individuals whose sensitive PII was improperly stored on the shared drive were not properly notified pursuant to DoD policy.

IO Findings: Notification Not Required Based On Low Risk Assessment.

Based on the additional policy guidance below a risk assessment has been conducted. The results indicate a "low" risk of harm to the individuals. With this "low" risk it is recommended the individuals should not be notified. Providing notification might create unnecessary concern and confusion that outweighs the risk of harm caused by the breach of information.

Additional policy guidance

a. Director, Administration and Management (DA&M) memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)" June 5, 2009

    (a) It shall be DoD policy that when making the determination of whether notification of breach is required, the DoD Component will assess the likely risk of harm caused by the breached information and then assess the relative likelihood of the risk occurring (risk level).

    (b) There are five factors that the DoD Component's will consider to assess the likely risk of harm. The DoD Component will consider a wide range of harms, such as harm to reputation and the potential for harassment or

[6] 1 May 2012, ITMD formerly a separate organization under WHS officially incorporated with OSD CIO to create EITSD.

prejudice, particularly when health or financial benefits information is involved in the breach. The DoD Component will bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

(c) Five factors to consider when assessing the likelihood of risk and/or harm:

1. Nature of the data elements breached.
2. Number of individuals affected.
3. Likelihood the information is accessible and usable.
4. Likelihood the breach may lead to harm.
5. Ability of the agency to mitigate the risk of harm.

b. DA&M memorandum "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations" August 2, 2012

(a) A final decision regarding whether to make notification cannot be made until after each factor has been assessed. The decision to notify should not be based on one factor alone. For example, a breach may involve social security numbers (SSNs) making that factor a high risk. However, SSNs may be stored on an encrypted, Common Access Card-enable laptop to mitigate potential compromise which could lead to harm. Therefore, although one factor in this example (data elements) rates as a high likelihood of hard, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place. Generally, absent other factors, Components should not notify personnel of breaches that have a low overall likelihood of harm.

Risk Assessment

FACTOR 1. Nature of the data elements breached.

The following PII data elements were identified in the five (5) documents provided by Ms. Brown-Richards:

1. Social Security Number
   In this instance the risk is considered LOW since access was by trusted DoD personnel on a DoD controlled information system (further explained in the factors that follow). There is no evidence to suggest the "public" had access to any PII, and there is no evidence to suggest a WHS employee intended to cause harm to any individual.

2. Date and Place of Birth

3. Personal email address

4. Personal home address and home phone number

5. Salary

6. Supervisor's cash award amount

FACTOR 2[7]. Number of individuals affected. 461[8]

FACTOR 3. Likelihood the information is accessible and usable.

This factor is considered LOW for the following reasons:

1. Access was by WHS personnel who are authorized on the EITSD controlled information system.

2. Access was unintentional and when discovered, reported to FSD management and EITSD personnel.

3. There is no evidence PII was accessed or used with malicious intent.

4. There is no evidence the PII was accessed by the public (out of DoD control).

5. There is no evidence of intrusion by non-authorized users to the EITSD managed network.

FACTOR 4. Likelihood the breach may lead to harm.

This factor is considered LOW for the following reasons:

1. There is no evidence of anticipated threats or hazards to the PII.

2. There is no evidence of anticipated harms (e.g. blackmail, loss of self-esteem) to the individuals.

3. WHS civilians on the EITSD network were previously determined suitable for Federal civilian employment based on at least a National Agency Check with Inquiries (NACI) which is the minimum requirement for non-sensitive positions.

4. Access to the EITSD network is restricted to those persons who meet Federal requirements for credentialing contained in Homeland Security Presidential Directive -12 and Federal Information Processing Standards Publication 201-1. Initial issuance of a Common Access Card requires, at a minimum, the completion of an FBI fingerprint check with favorable results and submission of a NACI to the Office of Personnel Management.

5. Cyber Awareness and Privacy Act training are required for new personnel and annually thereafter. Training reinforces the requirements and individual responsibility for safeguarding PII.

---

[7] The whistleblower alleged that members of the public are at risk. To date, there is no evidence that PII belonging to a member of the public has been breached.

[8] In total, 463 names were identified but two (2) names were duplicates, resulting in the correct count of 461.

FACTOR 5. Ability of the Agency to mitigate the risk of harm.

This factor is considered LOW for the following reasons:

1. Initial mitigation takes place prior to access to the EITSD network. As stated in Factor 4 of the risk assessment, NACI background checks are conducted before civilian employment and FBI fingerprint checks with submission of a NACI occur before granting access to the EITSD network. Anyone who does not favorably complete the required checks is not granted access to the network, mitigating the risk of harm.

2. With regard to PII on the shared drive, the following mitigation actions were taken:

    a. WHS personnel who found PII initiated the response and mitigation efforts by reporting the breach to FSD management and EITSD personnel.

    b. FSD Trusted Agents and EITSD personnel conducted a search of SPMD shared folders for PII. Files found were moved to a "quarantine" folder with access limited to the SPMD Trusted Agents.

    c. SPMD folders (now sanitized of PII), were move to an EITSD new network structure. SPMD personnel were reassigned to the network with access back to the former FSD shared drive eliminated.

4. SUMMARY OF EVIDENCE OBTAINED FROM THE INVESTIGATION

a. October 19, 2012, email from Mr. Luquette to Mr. Mayberry reporting that he (Luquette) found a document ("SPAD[9] Succession Plan") containing PII, on the shared drive.

    (a) Mr. Mayberry asks Ms. Brown-Richards if she can "fix this?"

b. October 19, 2012, email from Ms. Brown-Richards to FSD managers and FSD security that she found documents containing PII on the share drive. Ms. Brown-Richards further explains it appears some of the files may have been placed on the S drive for storage while others may have been compiled as the result of "some sort of computer glitch." Ms. Brown-Richards attached six (6) files, five (5) of which contained PII (described above where 461 individuals are identified). The 6th document was a DD Form 254[10] "DoD Contract Security Classification Specification" which does not contain PII.

c. October 22, 2012, email from Ms. Brown-Richards to FSD managers, FSD security and EITSD personnel, providing the file path name to 36 files containing PII.

---

[9] SPAD (Space Policy and Acquisition Directorate) is the previous name of SPMD.

[10] As stated in the letter from OSC, the whistleblower reported a document on the shared drive labeled "Top Secret." No actual classified document has been located on the shared drive. It is believed the whistleblower was referring to block 1a. of the DD Form 254 which lists Top Secret as "Facility Clearance Required" for the contractor listed in block 6a. of the same DD Form 254.

d. October 23, 2012, email from Ms. Brown-Richards to FSD security and EITSD personnel stating there are several hundred accessible folders she has not reviewed and others she may have missed. Ms. Brown-Richards states "I look forward to your updates and/or guidance."

e. November 27, 2012, email from Ms. Brown-Richards to FSD security and FSD managers where she provides a list of five (5) file names which contain PII.

f. November 28, 2012, email from Mr. Bill Nicholson, Deputy Director, SPMD, to FSD managers and FSD security, stating SPMD front office staff will continue efforts to eliminate any inappropriate documents only on the SPMD share drive. Additionally, FSD security (Mr. Luis Vazquez) will contact IT (EITSD) in regard to locking down the drives.

g. November 28, 2012, email from Mr. Ken Ballard, EITSD, to FSD managers and FSD security that he (Ballard) will contact Mr. Vazquez to determine the next steps.

h. November 30, 2012, email from Ms. Brown-Richards to FSD security and FSD managers notifying them of files containing PII (not her own) on her H[11] drive. Additionally she reported Mr. Ballard had asked her to "click" on a file which may have taken her outside of the SPAD folder.

i. January 17, 2013, email from Ms. Brown-Richards to FSD security, FSD management and WHS security stating, "I think a great deal of the folders and/or files have been removed or are no longer accessible, but there are still a multitude of documents that need to be addressed."

j. February 6, 2013, email from Ms. Becca Guerra, Space Management Specialist, SPMD notifies Ms. Brown-Richards of her PII (Ms. Guerra's) on the shared drive and requested it be removed. Ms. Brown-Richards further notifies FSD security, FSD managers and EITSD (Mr. Ballard). Ms. Brown-Richards added that Ms. Kobe Owens, Space Management Specialist, SPMD, reported finding PII of an employee assigned to Pentagon Force Protection Agency.

k. February 6, 2013, email from Ms. Brown-Richards to FSD security and SPMD managers that as part of the SPMD migration test pilot, had been migrated to Windows 7. This resulted in: new folder icons; inability to delete icons not recognized; a folder containing a multitude of files. Ms. Brown-Richards states she had notified Mr. Ballard, EITSD when she found files containing PII belonging to Ms. Tanya Rose[12], with Assistant Secretary of Defense Public Affairs. Ms. Brown-Richards stated when she later attempted to access the Tanya Rose file, it was no longer available. . Lastly, Ms. Brown-Richards observed a Z: drive, which she reported to Mr. Ballard.

[11] Each user of the information system is assigned to an "H" drive that is specific and accessible only to that user.
[12] Ms. Rose was a former employee of EITSD.

l. February 6, 2013, email from Ms. Karen Jewell, Space Management Specialist, SPMD, to Ms. Brown-Richards that she (Ms. Jewell) found her own PII on the share drive and requested it be removed. Ms. Brown-Richards subsequently notifies FSD security and SPMD managers.

m. A "print screen" of the AD files as viewed by Ms. Brown-Richards and the investigating officer on April 29, 2013. The AD files were viewed using the computer of Ms. Brown-Richards. Ms. Brown-Richards should not have had access to the AD files.

n. February 11, 2013, email from Ms. Brown-Richards to FSD security and SPMD managers that files containing PII are still accessible. Additionally, Ms. Brown-Richards suggested DoD Concessions Committee documents containing PII, be locked down.

o. One (1) Standard Form 180 "Request Pertaining to Military Records" containing PII of one individual.

p. One (1) Standard From 182 "Authorization, Agreement and Certification of Training" containing PII of one individual.

q. One (1) "Thrift Savings Plan Election Form" containing PII of one individual.

r. One (1) FSD memorandum, subject Recommendation for Supervisory Cash Award, containing the PII of one individual.

s. One (1) excel spreadsheet "DFD Alphabetical Civilian Locator Report" containing PII of 463 individuals.

t. May 3, 2013, email from Mr. Tony Smith EITSD to the Investigating Officer that he is the EITSD point of contact concerning this issue (OSC DI-13-0932)

u. May 6, 2013, email from Mr. Tony Smith to the Investigating Officer and EITSD personnel regarding action taken to prevent SPMD personnel from seeing other than PSMD folders. Mr. Smith described the following:

"Any scriptlogic rule that maps these users to these shares or any subfolders within them would fail. Users would not notice anything other than the absence of drive mapping they may have previously had. They would receive an "Access Denied" error if they attempted to manually browse the UNC path to the shares, or if they saved shortcuts to them."

"EITSD created a rule that denied SPMD/SPAD access to subfolders and files only, not the share itself. This would allow SPMD/SPAD users to continue mapping the share, but they would not be able to open any subfolders or files. EITSD removed the "deny" rule from the FSD SPAD, FSD SPMD, and SPMD folders only. They would be able to open these folders only."

With regard to receiving statements from EITSD personnel covering all activity, he (Mr. Smith) had not received any to date.

v. May 7, 2013, email from Mr. Ballard to the Investigating Officer and FSD security. Mr. Ballard states that during my (Investigating Officer) visit with Ms. Brown-Richards (April 29, 2013), PII was on the WHS root share, not FSD share folders. Ms. Brown-Richards and her supervisor could not access any FSD folders except SPMD. Mr. Ballard further states SPMD (users) can no longer see any other WHS data files.

w. May 10, 2013, word document, from Mr. Tony Smith to the Investigating Officer. Mr. Smith states that with regard to EITSD's previous knowledge of the FSD share drive issues, Mr. Michael Murphy (a former EITSD employee) and Mr. Ballard would have information. Mr. Smith recommended Mr. Ballard provide a timeline summary[13].

5. LISTING OF ANY VIOLATION OR APPARENT VIOLATION OF LAW, RULE, OR REGULATION

There is no evidence to suggest that anyone acted maliciously or intended to violate a law, rule or regulation, however:

a. Allegation 1:

WHS personnel who did not have an official "need to know" were able to access PII in shared folders on the EITSD network. This unauthorized access continued for several months as the exact cause within the network could not be identified and corrected. Although there is no evidence to suggest EITSD and FSD management intentionally failed to respond quickly and efficiently to mitigate the breach, the incident should have been given highest priority to resolve and effect mandatory notifications to WHS leadership and up to the DoD Defense Privacy and Civil Liberties Office.

a. DoD 5400.11-R, "DoD Privacy Program," C1.4.2.2., treat all unclassified records that contain personal information that normally would be withheld from the public under the Freedom of Information Exemption Numbers 6 and 7, as "For Official Use Only (FOUO)," and safeguard them accordingly.

b. DoDM 5200.01-V4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," Enclosure 3, d.(1): No person may have access to information designated FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose.

b. Allegation 2:

In October 2012 when the unauthorized access to PII was reported, the incident should have been treated as a breach and a risk assessment initiated to determine the risk of harm to individuals. A risk assessment was not initiated as the incident was not recognized as a breach since it had occurred within the EITSD controlled network. By signing into policy the Operating Instruction identified under Section 6 of this report, responsibilities and procedures are defined and will ensure all breaches are processed appropriately. The Operating Instruction assigns the responsibility to the Component Security Manager to ensure a risk assessment is conducted and provided to the Director WHS for review.

---

[13] A timeline has not been received.

a. DoD 5400.11-R, "DoD Privacy Program," DL1.10: A PII breach occurs when there is an "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected.

b. DA&M memorandum "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII):" DoD Components are to utilize the factors outlined in Appendix A and Table 1, or other approved methodology, to make determinations of risk of harm associated with a breach (loss, theft or compromise) of PII.

c. DA&M memorandum "Use of Best Judgment for Individual Personally Identifiable Information (PII) Breach Notification Determinations." This memorandum emphasizes "the Department must continue its efforts to promote a culture to continuously "think privacy" and act swiftly to develop and implement effective breach mitigation plans" ... "no two breaches of PII involve the exact same circumstances, personnel, systems, or information" ... "a case-by-case analysis combined with the use of best judgment is required for effective breach management" ... "the decision to notify should not be based on one factor alone" ... "for example, a breach may involve social security numbers (SSNs) making that factor a high risk" ... "however, SSNs may be stored on an encrypted, Common Access Card-enabled laptop to mitigate potential compromise which could lead to harm" ... "although one factor in this example (data elements) rates a high likelihood of harm, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place" ... "generally, absent other factors, Components should not notify personnel of breaches that have a low overall likelihood of harm" ... "notification when there is little or no risk of harm might create unnecessary concern and confusion" ... "overzealous notifications resulting from notification criteria which are too strict could render all such notifications less effective because consumers could become numb to them and fail to act when risks are truly significant."

6. DESCRIPTION OF ANY ACTION TAKEN OR PLANNED AS A RESULT OF THE INVESTIGATION

(A) Changes in agency rules, regulations or practices:

1. An Operating Instruction (OI) to respond to a privacy breach is in coordination. The OI assigns responsibilities and identifies procedures for immediate reporting of a breach, immediate response, and conducting of a risk assessment.

2. WHS will implement an annual review of shared folders on the EITSD network. The review will be used to reduce holdings of PII and ensure only authorized persons have access to the appropriate shared folder(s).

3. EITSD is developing new procedures and analyzing the feasibility of using password protection for any documents placed within organizational files.

(B) The restoration of any aggrieved employee:

Not applicable

(C) Disciplinary action against any employee

Although several employees and supervisors failed to follow regulations, I recommend that additional training and awareness programs be instituted instead of disciplinary action. This, along with signing into policy a breach response Operating Instruction, will increase awareness and assign responsibilities to afford a better response should a breach occur in the future.

(D) Referral to the Attorney General of any evidence of criminal violation:

Not applicable

Point of contact for this Report of Investigation is Mr. Thomas E. Prudhomme, WHS Security Manager, 571-372-0940.