

**Audit of NARA's Processing of
Military Personnel Record Requests
OIG Report No. 09-16**

September 30, 2009

EXECUTIVE SUMMARY

The National Personnel Records Center (NPRC) maintains the personnel and medical records of nearly all former members of the U.S. military service departments who served during the twentieth century. Approximately 80 percent of the records maintained by the National Archives and Records Administration (NARA) are the property of the Department of Defense, which reimburses NARA for storing and servicing the records. The remaining 20 percent have been accessioned as permanent records of the United States and are owned by NARA. In FY 2008, NARA's National Personnel Records Center (NPRC) had military service records for more than 56 million veterans. These records contained such documents as enlistment contracts, duty locations, performance evaluations, award citations, training records, and the Report of Separation (DD Form 214 or earlier equivalent)¹. NPRC responds to more than one million requests a year from veterans and their family members for information contained in the Official Military Personnel Files (OMPF).

For this audit, we assessed the management controls over the processing and distribution of veterans' record requests. Specifically, our review focused on whether the process was sufficient to properly safeguard veteran's information in accordance with the Privacy Act.

Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. The Privacy Act of 1974 required agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

We found that while NPRC has taken action to heighten the awareness of staff to erroneous disclosures² of veteran's information, controls over the processing of veteran's record requests need to be strengthened in order to properly safeguard veteran's PII. NPRC relies on an automated case management system to track and process both electronic and mail-based inquiries from receipt through fulfillment and closure. The system has significantly reduced the amount of time it takes NPRC to respond to a veteran's record request, however, vulnerabilities in the system leaves veteran's personal information susceptible to unauthorized disclosure and jeopardizes the integrity of the information stored in the system. We also found that additional safeguards are needed in order to protect veteran's PII in paper form and to ensure that persons requesting access to records have the proper authorization to obtain those records.

¹ The Report of Separation contains information such as dates and character of service, final rank, awards earned, and military occupation specialty. It is a key to obtaining veteran's benefits such as home loans, civil service appointments, education, training, and medical care.

² According to NPRC, an erroneous disclosure happens when a technician dispatches a response without properly verifying that the subject of the record matches the subject of the request or when a technician inadvertently switches response documents among service requests assigned to them.

This report contains 14 recommendations which upon implementation will assist NARA in providing appropriate administrative, technical, and physical safeguards over PII as required by the Privacy Act.

BACKGROUND

The National Personnel Records Center (NPRC) maintains the personnel and medical records of nearly all former members of the U.S. military service departments who served during the twentieth century, and responds to requests for these records. Most of the records maintained by NARA are the property of the Department of Defense (DoD), which reimburses NARA for storing and servicing the records. In 2004, DoD and the Archivist of the United States signed an agreement making the Official Military Personnel File (OMPF) a permanent record of the United States. In subsequent agreements, it was decided that an OMPF becomes archival and ownership transfers from DoD to NARA 62 years after the subject of the record was discharged or retired, or died in service.

NPRC receives approximately 4,000 requests per day about OMPF. Many of these requests come from veterans, their families, or organizations working on behalf of veterans to verify their military service, apply for benefits, or research medical conditions. More than 40 percent of the requests received ask for only a copy of the separation document, the DD Form 214 or its predecessor forms which contains important information such as dates and character of service, final rank, awards earned, and military occupation specialty. Other popular requests are to obtain copies of health records, replacement or newly authorized service medals, records of one's own (or a family member's) military service, and verification for entitlement for burial in a national cemetery. NPRC responds to more than one million requests a year and strives to answer all requests within 10 working days because a veteran's ability to obtain a job, housing, or medical care often depends on NPRC's ability to meet information needs quickly.

Federal law requires that all requests for records and information be submitted in writing. Each request must be signed (in cursive) and dated within the last year. To request military service records, veterans and the next of kin of deceased veterans may use one of the following methods:

- fill out an online request (using eVetRecs system);
- mail or fax a Standard Form 180;
- write a letter;
- visit NPRC; or
- hire an independent researcher.

In the FY 2008 Assurance Statement, NPRC officials reported they had increased their emphasis on protecting personal data but there were still 196 erroneous disclosures. According to NPRC officials, they take erroneous disclosures very seriously and when reported, will examine the circumstances surrounding the erroneous disclosure. When carelessness is determined to be the root cause, the erroneous disclosure is addressed with disciplinary actions. NPRC officials conducted a standardization review in FY 2008 which observed core technicians at work to determine their level of compliance with several critical tasks. The critical tasks were identified as actions that, if not taken, would have an extremely high likelihood of violating the Privacy Act, damaging record holdings, reducing the availability of essential documents, or providing a poor quality

response to the requester. An example of one critical task is that the technicians maintain only one record at a time in their immediate work area which would help correct the problem of technicians accidentally switching response documents among service requests assigned to them.

Safeguarding of PII is important to protect individuals, maintain public trust and confidence in an organization, protect the reputation of an organization and protect against legal liability for an organization. For Federal government agencies, the need to protect PII was first established by the Privacy Act of 1974. The Privacy Act required agencies to protect PII and to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

OJECTIVE, SCOPE, METHODOLOGY

The objective of this audit was to assess the management controls over the processing and distribution of veterans' record requests. Specifically, we determined whether the process was sufficient to properly safeguard veteran's information in accordance with the Privacy Act and OMB policies.

The audit was conducted at the National Personnel Records Center (NPRC) in St. Louis, MO and at Archives II in College Park, MD, primarily with the Office of Regional Record Services (NR) and the Office of Information Services (NH). We also contacted the Acquisition Services Division (NAA) and the General Counsel's Office (NGC).

In support of the audit objective, we reviewed the Privacy Act of 1974 and OMB policy memorandums on safeguarding PII. We also reviewed NARA policy and procedures for releasing veteran records. We evaluated controls over the receipt of military personnel record requests, the processing of those requests, and the distribution of the requested information to ensure privacy information was not released to unauthorized individuals. We evaluated controls in the Case Management and Reporting System (CMRS) to determine whether the controls were reasonable to protect the confidentiality of data against such risks as unauthorized access, modification, or disclosure of data. We also reviewed additional physical security controls in place to protect veteran's privacy information.

We interviewed NPRC officials, observed the process of receiving military personnel record requests and responding to those requests, examined technical and operational controls in the Case Management and Reporting System, and reviewed pertinent documentation to determine whether veteran's information is appropriately safeguarded.

Our audit work was performed between January 2009 and August 2009. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and

conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS AND RECOMMENDATIONS

Controls over Information in the Case Management and Reporting System

Our review found that controls over information in CMRS were not adequate to safeguard the confidentiality of PII or the integrity of the information stored in the system. Specifically weaknesses exist in access controls, controls over data extracts containing sensitive PII, the protection of data stored on mobile devices, and the type of encryption used for remote access to the system. These weaknesses exist because NPRC officials, as the system owner, did not implement effective controls. The Privacy Act of 1974 requires NARA to maintain appropriate safeguards over the PII data stored in the system. As a result, NARA faces an increased risk of inappropriate disclosure of PII or destruction to the data in CMRS.

According to the Privacy Act of 1974, each agency that maintains a system of records shall establish appropriate administrative, technical and physical safeguards to assure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. NARA maintains a system of records for the automated CMRS and therefore, is responsible for establishing appropriate controls to safeguard the information.

Data Stored in the System

The CMRS database includes all record requests submitted to NPRC since the system went into operation in October 2002. Therefore, over seven million record requests were stored in the CMRS database. Although a records disposition schedule to delete requests in the CMRS database was approved, NPRC officials did not follow the schedule and saved all requests. According to OMB Memorandum 07-16, one way to reduce the risk related to a data breach was to reduce the volume of collected and retained information to the minimum necessary. Maintaining unnecessary record requests in the database increases the potential damage that could be caused if a data breach were to occur since each record request contains PII.

CMRS includes an online service request and record tracking database. This database tracks and processes both electronic and mail-based inquiries from receipt through fulfillment and closure. Upon receipt, new cases are input electronically and physical documents are converted into digital images. Information entered into the system includes the requester's name, address, and phone number as well as the veteran's full name, social security number, date of birth, place of birth, and branch of service. Figure 1 is a view of the CMRS service request input screen to demonstrate the information entered into the system. While all personal information about the veteran does not have to be filled in, requesters are encouraged to provide as much information as possible in order to ensure the correct record is found. The CMRS database is archived to keep a permanent transaction record of the service provided.

Source: CMRS Concept of Operations

Figure 1. CMRS Service Request Input

As shown in Figure 1 above, the CMRS system contains all the information needed to steal a veteran’s identity. For example, if a veteran were to request a copy of the records of their military service, the CMRS database would store their name, current address, and phone number in the Requester Information fields, and their social security number, date of birth and place of birth in the Veteran Information fields.

According to the Records Disposition Schedule:

- Transaction data gathered and/or generated as the result of receiving and processing a customer request (including name of requester, name of veteran whose data is being requested, images of requester documentation, etc) should be cut off at the end of each fiscal year and can be destroyed 5 years after the cutoff.
- Transaction data for access information (an extract of the live transaction data including name of veteran whose data is being requested, date requested, name of requester and associated records block) should be cut off at the end of each fiscal year. Data associated with these requests are exported to a "record of disclosure file" external to CMRS.

According to an NPRC official, completed record requests have not been removed from CMRS because when working on cases, technicians often have to refer to previous cases. However, one technician interviewed stated they do not use earlier cases in CMRS

because there is no way to search by case type to find how a similar request was answered. In addition, the technician stated each record request is unique, and therefore earlier cases would not be very useful. Another technician stated they refer back to previous cases in CMRS only when the case assigned is coded by CMRS as a duplicate. In those instances, the technician stated they would review the prior case to determine why another request was submitted.

A breach or loss involving this data could be very damaging financially and could erode public confidence, potentially jeopardizing NPRC's ability to achieve its mission. Additionally, if the breach constitutes a violation of relevant law, NPRC and/or its staff may be subject to criminal or civil penalties.

Recommendations

1. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to export data for the "record of disclosure file" and follow the approved Records Disposition Schedule and limit the amount of record requests stored online.

Management Comments

Management concurred with the recommendation.

Password Configuration Weaknesses

A username and password were needed to log into the CMRS system however, password requirements were not in place to protect the confidentiality of passwords and prevent unauthorized access. This occurred because NPRC officials did not believe password requirements were needed. NIST SP 800-53 requires information systems to uniquely identify and authenticate users and NARA Interim Guidance 804-2, requires all passwords for unclassified systems must be at least 8 characters and include special characters such as punctuation marks or symbols. Weak passwords increase the risk that an unauthorized person could gain access to information stored in the system.

User authentication establishes the validity of a user's claimed identity. The most widely used means of authentication is through the use of passwords. However, passwords are not conclusive identifiers of specific individuals since they may be guessed, copied, overheard, or shared. Therefore, additional controls are needed to protect the confidentiality of passwords. NPRC officials did not implement necessary controls to protect the confidentiality of CMRS passwords. Specifically:

- ----Redacted pursuant to FOIA Exemption "high" b(2)----;
- ----Redacted pursuant to FOIA Exemption "high" b(2)----;
- ----Redacted pursuant to FOIA Exemption "high" b(2)----;
- ----Redacted pursuant to FOIA Exemption "high" b(2)----;

- ----Redacted pursuant to FOIA Exemption "high" b(2)----; and
- ----Redacted pursuant to FOIA Exemption "high" b(2)----.

 -----Redacted pursuant to FOIA Exemption "high" b(2)-----

According to NPRC officials, stronger password requirements were not needed because physical security controls at the facility would prevent an unauthorized user from gaining access to a computer terminal at NPRC. In addition, a user would need to have a NARANET account and a Windows domain account in order to gain access to the system. While physical security controls and the need for a NARANET account provide additional layers of security, these controls do not protect the confidentiality of the passwords.

-----Redacted pursuant to FOIA Exemption "high" b(2)-----

Recommendations

2. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to establish and enforce password requirements within CMRS that are appropriate based on the sensitivity of the information contained in the system and the need to protect the integrity of the information.

Management Comments

Management concurred with the recommendation.

Audit Response

Although the Assistant Archivist concurred with the recommendation, discussions about the draft report with management indicated the technical solution would not be implemented until ----Redacted pursuant to FOIA Exemption "high" b(2)----. We do not agree that implementation should be delayed until ----Redacted pursuant to FOIA Exemption "high" b(2)----. The current CMRS system has the capabilities to enforce password requirements therefore, ----Redacted pursuant to FOIA Exemption "high" b(2)---- results in unnecessary risk to the confidentiality of data in the system.

Least Privilege

Over 50 Data Entry Clerks were given full access to the entire CMRS database and over 250 Core Technicians responding to record requests have the ability to view all requests in the database. This occurred because controls were not in place to enforce the most restrictive set of rights and privileges needed by users in performing their jobs. As a

result, information in the system was not protected against unauthorized access, modification, loss, or disclosure.

Data Entry Clerks are responsible for entering data from record requests received by mail into the CMRS system and then scanning a copy of the request which is saved as an attachment to the record request. In February 2009 there were 39 Data Entry Clerks as well as an additional 18 employees that perform other duties at NPRC but work overtime in the mailroom as Data Entry Clerks. Data Entry Clerks were granted access to the entire database of record requests and had the ability to edit all record requests.

According to an NPRC official, data entry clerks need access to the all service requests because occasionally, a re-scan of the original record request is needed. In those instances, a re-scan notice is received from the mailroom supervisor and the assigned data entry clerk is to retrieve the original service request from storage and re-scan the request. The data entry clerk performing the re-scan is not always the original clerk who entered the data. The ability of data entry clerks to edit all requests increases the risk that a data entry clerk could intentionally or unintentionally delete or modify any record requests. The intentional or unintentional deletion or modification of incoming record requests could severely impact operations at the NPRC.

Core Technicians are responsible for reviewing the requests assigned to them, determining the information that should be provided and then responding to the request. While Core Technicians are only able to edit those requests assigned to them, the ability of more than 250 core technicians to view sensitive PII information in all requests stored in the system increases the risk of an inappropriate disclosure of data.

Recommendations

3. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to establish controls to restrict users to only those rights and views needed to perform their job.

Management Comments

Management concurred with the intent of the recommendation but believed that appropriate controls consistent with business needs have been in place since 2002. Therefore, the Assistant Archivist does not anticipate making any changes and will accept this business risk.

Audit Response

Although the Assistant Archivist concurred with the intent of the recommendation, we do not agree with their plan to not take action to limit the set of rights and views of CMRS users. NARA can safeguard the confidentiality of PII by ensuring that users who must access records containing PII only have access to the minimum amount of PII data, along with those privileges (i.e. read, write, execute) that are necessary to perform their duties.

Review of System User Accounts

We identified several user IDs no longer in use that had not been removed from the system. This occurred because periodic reviews of the user ID's were not adequate to detect user accounts no longer needed. According to NIST SP 800-53, information system accounts should be reviewed at least annually. If user IDs no longer in use are not removed promptly, information in the system is at a greater risk of unauthorized disclosure.

In a review of CMRS user accounts we identified seven generic user ID's including four with administrative access. We requested additional information from NPRC as to what the accounts were used for. We also identified four NARA IT employees who had user accounts but no longer required access to the system. One of the four employees retired from NARA in January 2008 and returned to NARA as a contractor in February 2008 but their user ID was not removed even though access to CMRS was no longer needed. According to an NPRC official, a total of eight user ID's were no longer needed and would be deleted.

According to an NPRC official, they are not able to delete user accounts in CMRS but they are able to remove the "views" assigned to that person. The CMRS contractor is responsible for deleting the CMRS database account. According to the NPRC official, the eight user IDs that were determined to no longer be needed were probably established when the system was first developed and NPRC officials were not notified that the user accounts were no longer needed.

Recommendations

4. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to review all application and database users at least annually.

Management Comments

Management concurred with the recommendation.

Controls over Data Extracts Containing Sensitive PII

CMRS users were not restricted from performing extracts of the database which could contain sensitive PII and ----Redacted pursuant to FOIA Exemption "high" b(2)----. In addition, the creation of computer-readable extracts from CMRS containing PII ----Redacted pursuant to FOIA Exemption "high" b(2)----. This occurred because 1) ----Redacted pursuant to FOIA Exemption "high" b(2)----; 2) ----Redacted pursuant to FOIA Exemption "high" b(2)----; and 3) ----Redacted pursuant to FOIA Exemption "high" b(2)----. OMB Memorandum 06-16 required -----
-----Redacted pursuant to FOIA Exemption "high" b(2)-----
----- Without ----Redacted pursuant to FOIA Exemption "high" b(2)----, veteran's data is at an increased risk of disclosure.

A computer-readable data extract from a database involves retrieving data from a database through a query and saving the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file. According to an NPRC official, every CMRS user has the ability to perform a query of information in the CMRS database, which includes sensitive PII. -----

-----Redacted pursuant to FOIA Exemption "high" b(2)-----.

According to a CMRS official, they were aware of only two extracts of the CMRS database where information was queried and then saved to a CD. The CMRS official stated that these extracts were provided to the Marine Corps in July 2008 and January 2009. The extracts were logged by the CMRS official using email however, the official was only able to provide emails relating to the second data extract due to the loss of their email archives. Therefore, email should not be used as a means of tracking data extracts.

-----Redacted pursuant to FOIA Exemption "high" b(2)-----

Recommendations

5. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to limit users' ability to perform extracts of the database containing sensitive information or remove access to CD burners and thumb drives.

Management Comments

Management concurred with the intent of the recommendation stating system stakeholders are reviewing options for a technical and non-technical solution.

6. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to -----

-----Redacted pursuant to FOIA Exemption "high" b(2)-----.

Management Comments

Management concurred with the intent of the recommendation stating that they will review options for a solution that will be tied to the technical refresh. The solution will take into consideration technical feasibility, cost, and performance implications.

Protection of Data Stored on Mobile Devices

CMRS backup tapes containing sensitive information were not encrypted before they were sent to an offsite storage facility or shipped to NPRC. This occurred because NARA did not have an encrypted file system. OMB 06-16 requires agencies to encrypt all data on mobile devices which carry agency data unless the data is determined to be

non-sensitive. If sensitive data is not encrypted, NARA faces an increased risk that the information could be disclosed to unauthorized individuals if the tapes are lost or stolen.

The intent of encrypting mobile devices is to protect sensitive information when it is removed from the agency's secured physical perimeter. According to a NARA Privacy Official, encryption of mobile devices includes backup tapes since the tapes are removed from the facility. Weekly full backups of the CMRS system are made and then sent to an offsite storage facility. In addition, backup tapes of closed record requests are shipped periodically to NPRC in St. Louis for storage. None of the backup tapes were encrypted.

According to an NH official, NARA is in the process of obtaining an encrypted file system. Until backup tapes are encrypted, sensitive data on the backup tapes are vulnerable to loss or theft while in transit to the offsite storage facility and to NPRC.

Recommendations

7. The Assistant Archivist for Information Services should encrypt backup tapes containing PII as required by OMB Memorandum 06-16.

Management Comments

Management concurred with the intent of the recommendation stating controls related to protecting PII with encryption are covered in NARA Directive 1608.9 and possible solutions will be considered as part of the technical refresh.

Encryption Used for Remote Access to the CMRS System

CMRS contractors use NARA's Virtual Private Network (VPN) to remotely access the system servers and their workstations. However, weaknesses in NARA's VPN results in risks to the confidentiality of the information accessed remotely. This occurred because -----Redacted pursuant to FOIA Exemption "high" b(2)-----

Without secure remote access, information transmitted may be disclosed to unauthorized parties.

A VPN is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data. According to NIST, VPNs are used most often to protect communications carried over public networks such as the Internet. One way organizations can protect the confidentiality of transmitted PII is to encrypt the communications. Any information that will cross over the VPN connection that is not to be seen by non-VPN users should be encrypted to provide confidentiality protection for that information.

CMRS contractors use NARA's VPN to remotely access the system servers and their workstations. According to the contractor, remote access is needed to perform routine tasks and respond to other issues after hours. However, weaknesses in NARA's VPN results in risks to the confidentiality of the information accessed remotely. Specifically, the -----
-----Redacted pursuant to FOIA Exemption "high" b(2)-----

 Another risk to the confidentiality of information transmitted over the VPN connection is that CMRS contractors are ----Redacted pursuant to FOIA Exemption "high" b(2)----³ ----
 -----⁴ Allowing ----redacted---- increases the risk of disclosure of data in
 CMRS because it allows ----Redacted pursuant to FOIA Exemption "high" b(2)----. ----
 -----Redacted pursuant to FOIA Exemption "high" b(2)-----

 ----- According to the CMRS contractors, they could use a more secure
 protocol to access the CMRS servers however, the protocol would have to be installed on
 every server. -----Redacted pursuant to FOIA Exemption "high" b(2)---

CMRS contractors use the free version ---redacted--- to access the servers from their
 desktop computers at NARA and to access their workstations when working remotely.
 The contractor was aware of the security concerns involved ----Redacted pursuant to
 FOIA Exemption "high" b(2)---- but stated its use was approved by the Office of
 Information Services (NH). According to the contractor, NH performed security scans on
 the server configurations in 2004 and did not disallow its use therefore, they continue to
 use it. According to -----Redacted pursuant to FOIA Exemption "high"
 b(2)----- is unencrypted and anything typed into the viewer passes "in the
 clear" to the server. While the free edition may be suitable for use within NARANET or
 with a secure VPN, it should not be used in conjunction with NARA's VPN to access
 sensitive information contained in the CMRS system. CMRS officials should either -----
 -----Redacted pursuant to FOIA Exemption "high" b(2)----- to ensure information
 transmitted remotely is not disclosed to unauthorized parties.

Use of ----Redacted pursuant to FOIA Exemption "high" b(2)---- was recorded as a
 weakness on the ----Redacted pursuant to FOIA Exemption "high" b(2)----. The
 weakness was listed as "ongoing" with an original scheduled completion date of May 31,
 2007. Due to the sensitivity of information contained in the CMRS system, ----Redacted
 pursuant to FOIA Exemption "high" b(2)----.

Recommendations

8. The Assistant Archivist for Information Services should use encryption that is FIPS 140-2 certified for the VPN.
9. The Assistant Archivist for Information Services should remove ----Redacted pursuant to FOIA Exemption "high" b(2)---- from the CMRS servers and install a more secure protocol.

³ ----Redacted pursuant to FOIA Exemption "high" b(2)----.

⁴ ----Redacted pursuant to FOIA Exemption "high" b(2)----.

10. The Assistant Archivist for Information Services should determine whether use of ---Redacted pursuant to FOIA Exemption "high" b(2)--- is needed, and if so, upgrade to a more secure version.

Management Comments

Management concurred with the recommendations.

Unresolved Server Security Vulnerabilities

The quarterly vulnerability scan of the CMRS servers in February 2009 identified:

- 18 critical confirmed vulnerabilities that allow ---Redacted pursuant to FOIA Exemption "high" b(2)---. Examples are the ability to -----Redacted pursuant to FOIA Exemption "high" b(2)-----; and
- 21 high confirmed vulnerabilities that -----Redacted pursuant to FOIA Exemption "high" b(2)---. Examples are -----Redacted pursuant to FOIA Exemption "high" b(2)-----; and
- 107 medium confirmed and potential warnings that have the potential of granting access or allowing code execution by means of -----Redacted pursuant to FOIA Exemption "high" b(2)-----. Examples are -----Redacted pursuant to FOIA Exemption "high" b(2)-----.

The confirmed vulnerabilities represent exploitable security problems that compromise confidentiality, integrity and availability. These vulnerabilities result in security weaknesses that must be fixed. As of June 2009, action had not been taken to correct these vulnerabilities. This was because the CIO's office believed the results were not accurate and because there was difficulty in tracking the IP addresses noted on the reports to the actual equipment. Delays in investigating these vulnerabilities could severely impact the confidentiality, integrity and availability of the CMRS system.

Recommendation

11. The Assistant Archivist for Information Services should review these vulnerabilities and determine whether action is needed.

Management Comments

Management concurred with the recommendation.

Verification for Next of Kin Requests

NPRC does not require technicians to perform any verification to confirm that the veteran is deceased before releasing records to next-of-kin requests. NPRC officials stated that DoD has not provided any additional funding to cover the cost of making these verifications, and therefore no changes have been made. The DoD Privacy Office stated that if the personnel file does not reflect that the member is deceased, the individual requesting such access should be required to provide reasonable proof that the member is deceased. In addition, the SF-180 form instructions state that for next of kin requests, the requester must provide proof of death. If NPRC does not perform proper verification, individuals may be granted unauthorized access to military personnel records.

The SF-180 form is used to request information from military records. Release of the information is subject to restrictions imposed by the military services consistent with DoD regulations and the provisions of the Freedom of Information Act and the Privacy Act of 1974. A veteran's next of kin can only request a record if the veteran is deceased however, NPRC does not require the requester to submit proof that the veteran is deceased. The instructions on the SF-180⁵ states that for next of kin requests, the requesters must provide proof of death, such as a copy of a death certificate, letter from funeral home or obituary. However, NPRC does not enforce this requirement. According to the NPRC 2008 Annual Assurance Statement, when responding to requests from the next of kin of deceased veterans, NPRC accepts the requester's signature as certification that they are authorized requesters.

The Department of Defense Privacy Office sent a letter to the NPRC Director in November 2007 regarding the release of records to the next of kin (NOK) when the NOK reports that a former member is deceased. According to the Defense Privacy Office, it is essential that both the relationship to the individual and proof of death be established before providing access and/or releasing the record to the NOK. If the military personnel file does not reflect the requester as a NOK, then the individual should be required to provide reasonable proof of his or her identity and relationship to the individual. Similarly, the Defense Privacy Office states that if the personnel file does not reflect that the member is deceased, the individual requesting such access should be required to provide reasonable proof that the member is deceased.

The NPRC Director estimated that approximately 15 additional people would need to be hired to review the NOK requests and obtain the required documentation to verify the veteran was deceased and establish the relationship of the requester to the veteran. The cost of this change along with other changes mentioned by the Defense Privacy Office was estimated to be \$8.5 million annually. Therefore, the Director proposed an alternative solution which he determined would cost significantly less. The alternative was to require verification of the veteran's death but continue to use the perjury statement and technician review to establish the NOK relationship. According to the NPRC

⁵ The requirement for requesters to provide proof of death was added in the September 2008 revision of the SF-180 form.

Director, the Defense Privacy Office never responded to his letter and did not fund the cost of making these verifications therefore, no changes have been made to the process.

The Privacy Act states that agencies are not to disclose of any record to any person or to another agency without a written request by or with the prior written consent of the individual to whom the record pertains⁶. One core Technician interviewed stated that for NOK requests they would review the social security index or the Department of Veterans Affairs Beneficiary Identification Records Locator Subsystem (BIRLS) database to verify whether a veteran was deceased before responding to a NOK request. NPRC should ensure that the NOK requesting records has the proper documentation in order to prevent unauthorized access to military personnel records.

Recommendations

12. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to issue policy that requires technicians to verify that the veteran is deceased before providing military records to a next of kin.

Management Comments

Management concurred with the recommendation.

Additional Safeguards Needed to Protect PII in Paper Form

Although controls were in place to protect military records stored in the stack areas, over 40,000 military records were left out in the office areas overnight and the Facility Manager was unsure as to how many individuals had a copy of the master key needed to open these doors. This occurred because keys were not returned when individuals left and annual key inventories were not conducted. According to NARA 271, NPRC should have a key control plan to maintain a high level of security at the facility. Specifically, a Key Control Officer should determine which keys, based on need, to issue to each employee, and carry out or oversee completion of the required inventories of keys issued and retained. Without proper key control, NPRC risks unauthorized access to military records or disclosure of PII.

NARA Directive 1608 states that if staff collect, maintain, or disseminate PII in the course of performing their duties, they must ensure that the information is properly protected. During normal business hours, maintain information in areas accessible only to authorized individuals. After business hours, offices that collect or maintain PII must be locked. When not in use, paper based records containing PII must be stored in locked cabinets.

⁶ The Privacy Act contains twelve conditions on which information could be disclosed without the consent of the individual. For example, records could be disclosed pursuant to the order of a court of competent jurisdiction.

Staff at NPRC collect, maintain, and disseminate PII in the course of performing their duties. Therefore, PII is throughout NPRC offices and because of the nature of the operations, there are substantial amounts of it. On March 26, 2009, there were approximately 29,000 records in the Record Retrieval Area waiting to be re-filed and approximately 15,000 records out in the Core Technician areas.

For example, stacks of incoming mail with veteran's record requests were located in the mailroom. As shown in Figure 2, completed record requests were also kept in the mailroom, waiting for pickup by the U.S. Postal Service (USPS). Completed requests received after the USPS pickup would be stored in the mailroom overnight. According to a mailroom supervisor, the doors to the mailroom are closed and locked when the last person leaves for the day.

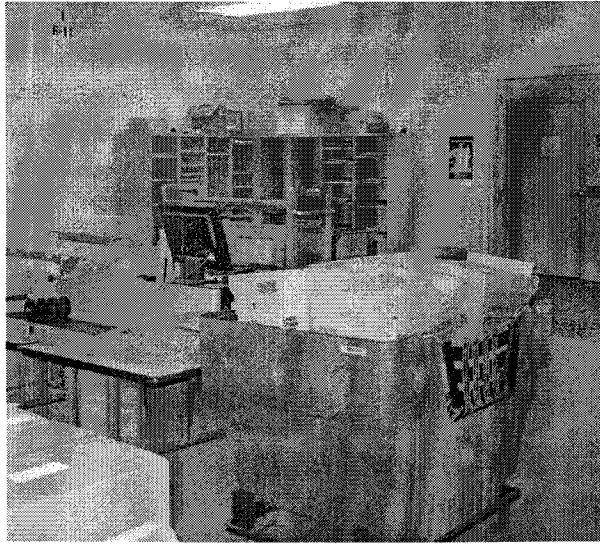


Photo Taken by NPRC

Figure 2. NPRC Record Request Responses.

Each Core Technician has a cubicle with a desk and a cart (see Figures 3 and 4). The cart is used to organize the OMPF's of the cases they are working on. Core Technicians do not secure PII located on their desk or cart when they are away from their desk or when they leave for the day. Instead, the doors to the area were closed and locked.



Photo Taken by NPRC

Figure 3. Core Technician Desk Cart



Photo Taken by NPRC

Figure 4. Core Technician Cubicles

In the Records Retrieval Branch there were carts full of military records waiting to be re-filed (as shown in Figure 5 and 6). The doors into the Record Retrieval Branch were closed and locked by the last person to leave.

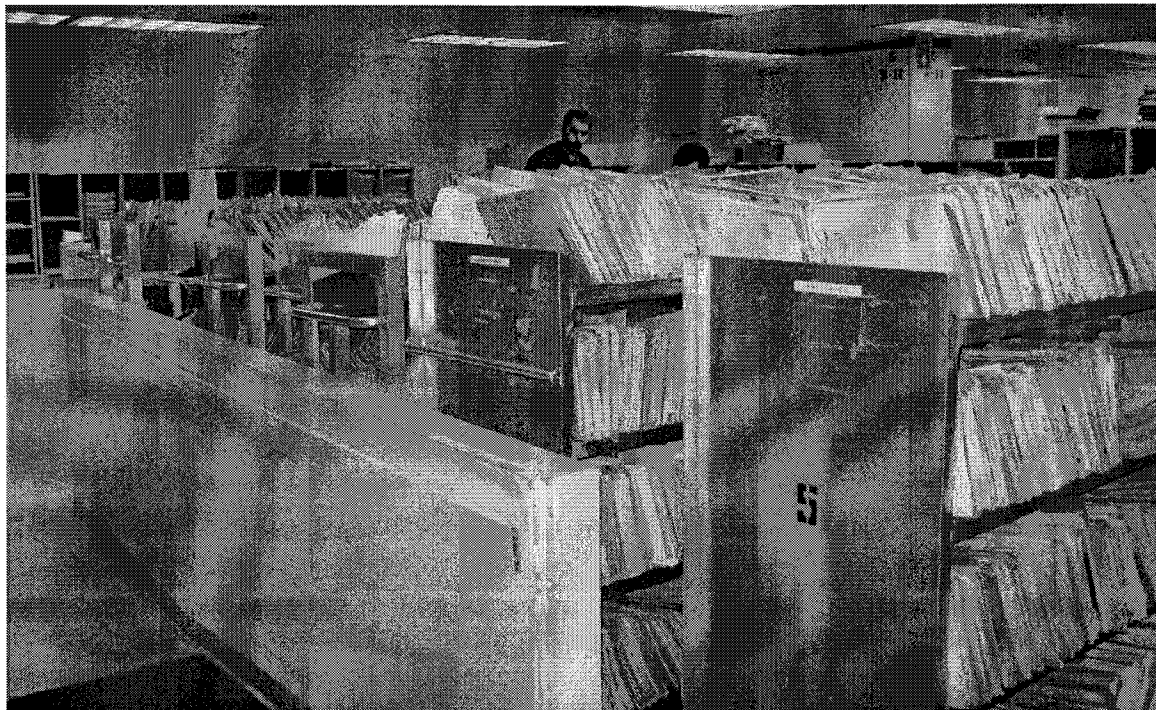


Photo Taken by NPRC

Figure 5. OMPFs Returned and Waiting to be Re-filed.

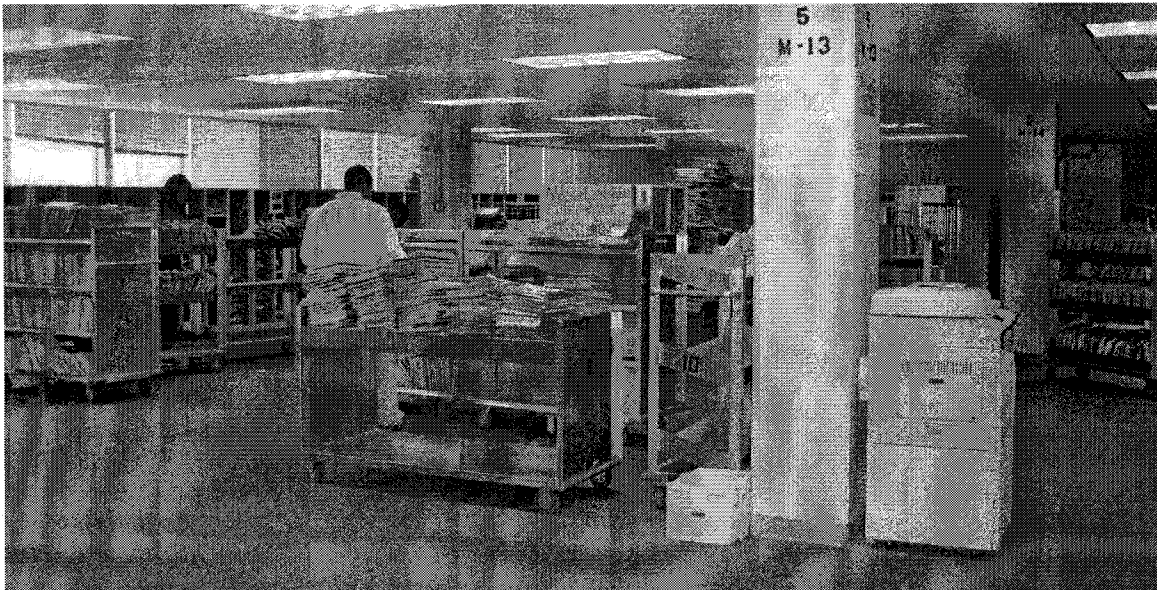


Photo Taken by NPRC

Figure 6. Staff organizing OMPFs to be re-filed.

Based on the office layout at NPRC, it was not possible for all the records to be stored in locked cabinets as required by NARA Directive 1608. In addition, an NPRC official stated that they would not want technicians to be able to lock up records in their desks.

The --redacted-- key opens all the doors to these office areas. For example, a mailroom employee would be able to unlock the door and obtain access to the Records Retrieval Branch. The Facility Manager stated he performed a key inventory in 2005 and estimated there were ----redacted---- keys. However, the key inventory consisted of sending an email to each of the core managers and asking them to report how many keys they had issued to their staff therefore, additional master keys may exist. According to the facility manager, no keys have been turned back in to him since he performed the key inventory in 2005. The facility manager believed that instead of turning in keys to his office when staff leave, supervisors keep the key to hand out to the next person.

Physical access controls are designed to protect the organization from unauthorized access. These controls should limit access to only those individuals authorized by management. Further, all keys should be accounted for and not left with former employees or contractors. Without adequate key control, NPRC is vulnerable to physical access exposures including damage, vandalism or theft of equipment; copying or viewing of sensitive information; and alteration of sensitive equipment and information. Possible threats include employees with authorized or unauthorized access who are disgruntled, threatened by disciplinary action or dismissal, addicted to a substance or gambling, experiencing financial or emotional problems, or notified of their termination.

NPRC will be moving to a new facility in 2010 however, in the interim, a key control inventory of the NARA10 key and any other master keys should be conducted.

Recommendations

13. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to conduct a key inventory of the --redacted-- key and any other master keys in use at NPRC to ensure all keys are accounted for.

Management Comments

Management concurred with the recommendation stating that the required key inventory has been completed.

Paper Recycling

NPRC used contractor-witnessed pulping to dispose of its waste paper containing PII and did not shred paper prior to pickup by the contractor. This occurred because NPRC did not have shredders with the capacity to handle the volume of paper with PII being recycled and because NPRC officials decided to treat paper with PII in the same manner in which restricted records center holdings are disposed. NARA Directive 1608 requires staff who collect, maintain, or disseminate PII in the course of performing their duties, to properly destroy materials containing PII. As a result, NPRC waste paper containing PII may be disclosed to unauthorized individuals and due to the sensitivity of information contained on the paper, could lead to identity theft.

According to NARA Directive 1608, if staff collect, maintain, or disseminate PII in the course of performing their duties, they must ensure the information is properly protected. Specifically, NARA staff are to properly destroy materials containing PII by shredding, burning, deleting or other authorized destruction methods that ensures the data or record is unreadable or unrecoverable.

NPRC has a recycling contract for disposal of their paper. NPRC decided to enter into their own contract, separate from GSA, because so much of the paper they recycle has PII. For example, all record requests received in the mail are recycled. Information that may be included on the record request form include the veteran's: full name, social security number (SSN), service number (SN), place of birth, and date of birth. In addition, the CMRS system prints out Search Request forms (shown in Figure 7 below) which may include the veteran's name, SSN, SN, place of birth and date of birth. These papers are placed into large yellow bins to be recycled (see Figure 8 below).

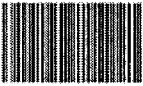
NPR Search Request		NPRC	
National Archives and Records Administration			
Priority: Routine		 1-2MPA269	
Source: Routine			
Complexity: Separation Doc			
Search Type: 1st Search			
Non-Registry Block:			
Registry Number:			
Reg Veteran's Name: [REDACTED]		SR Number:	
SR Veteran's Name: [REDACTED]		Search Section: 3	
SSN: [REDACTED]		S E P D	
DOB: [REDACTED]			
POB: [REDACTED]			
SSN/SVN: [REDACTED]			Core: Core 1
Service Code: AR			Team: Team E
Service Number:			
Record Charged to:			

Figure 7. Example of a Search Request

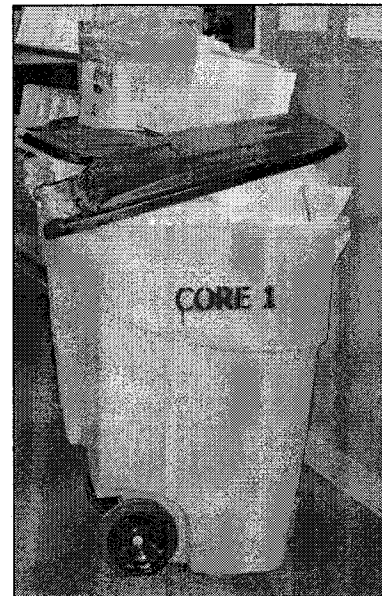


Photo Taken by NPRC

Figure 8. Paper Recycle Bin

According to the contract, the method of destruction would be repulping and a representative of the contractor would witness the loading and sealing of the enclosed van trailer, which would be sent to a recycling mill in Oklahoma. According to the contract, once the contractor receives written notification the material has been destroyed through the process of re-pulping, a Certificate of Destruction is issued. The contract does not specify that a representative from the contractor will witness the destruction of the paper, only the loading and sealing of the truck at NPRC. Although the Performance Work Statement states that the government has the right to send its representatives into the offices and plants of the contractor of those facilities utilized by the contractor for destruction for the purpose of verifying terms of the agreement are met, NPRC officials have not inspected the re-pulping facility since the issuance of the contract.

An NPRC official stated that some managers have shredders in their offices which they use for shredding personal and/or sensitive materials, but because so much of the NPRC office waste includes PII it is handled in the same manner in which the disposal of restricted records center holdings are handled; witness disposal by pulping in accordance with NARA 1464 "Destruction of Federal Records in the Custody of NARA Records Centers." According to NARA 1464, if the records are restricted, the wastepaper contractor must be required to pulp, macerate, or shred the records, and their destruction must be witnessed by either a Federal employee or, if authorized by the agency that created the records, by a contractor employee.

Recommendations

14. The Assistant Archivist for Regional Records Services should direct the Director, NPRC, to periodically inspect the recycling mill to ensure requirements of the contract are being met and that the sealed truck is stored in a secure area until the paper can be recycled.

Management Comments

Management concurred with the recommendation.



National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: September 30, 2009

To: Office of the Inspector General (OIG)

From: Policy and Planning Staff (NPOL)

Subject: OIG Draft Report No. 09-16, Draft Audit of NARA's Processing of Military Personnel Record Requests (CMRS)

Thank you for the opportunity to review and comment on this draft audit report. We appreciate the efforts of your staff and all parties associated with the audit process. This memo contains the combined comments of NR, NH, and NGC. We concur with the majority of the 14 recommendations as detailed below and we appreciate the auditor's willingness to work with the language in the audit and recommendations.

We concur with recommendations 1, 2, 4, 8, 9, 10, 11, 12, and 14, some of which require a technical solution. We will include additional information on these in our action plan. We also concur with recommendation 13. NR notes that the required key inventory has been completed.

We concur with the intent of recommendation 3. However, appropriate controls consistent with NR business needs have been in place since 2002. No changes are anticipated, and management will accept this business risk in our action plan.

We concur with the intent of recommendation 5. There are business reasons for performing extracts of data in the system, and controls are covered in NARA 1608, Protection of Personally Identifiable Information. System stakeholders are reviewing options for a technical and non-technical solution.

We concur with the intent of the recommendation 6. System stakeholders will review options for a solution that will be tied to the technical refresh. The solution will take into consideration technical feasibility, cost, and performance implications.

We concur with the intent of recommendation 7. Controls related to protecting PII with encryption are covered in NARA 1608.9. Possible solutions will be considered as part of the technical refresh.

If you have questions about these comments, please contact Mary Drak at 301-837-1668 or by email at mary.drak@nara.gov.

A handwritten signature in cursive script that reads "Susan M. Ashtianie".

SUSAN M. ASHTIANIE
Director, Policy and Planning Staff