

Naval Audit Service



Audit Report



Management Controls of Navy Corporate Data

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

~~Do not release outside the Department of the Navy,
post on non NAVAUDSVC Web sites, or in Navy Taskers
without prior approval of the Auditor General of the Navy.~~

N2015-0026
16 July 2015

**Obtaining
Additional Copies**

To obtain additional copies of this report, please use the following contact information:

Phone: (202) 433-5757

Fax: (202) 433-5921

E- NAVAUDSVC.FOIA@navy.mil

mail: Naval Audit Service

Mail: Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC
20374-5005

**Providing Suggestions
for Future Audits**

To suggest ideas for or to request future audits, please use the following contact information:

Phone: (202) 433-5840 (DSN 288)

Fax: (202) 433-5921

E- NAVAUDSVC.AuditPlan@navy.mil

mail: Naval Audit Service

Mail: Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-
5005

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

<http://www.secnav.navy.mil/navaudsvc>



DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
2013-064
16 July 15

MEMORANDUM FOR THE DEPUTY, CHIEF OF NAVAL PERSONNEL

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

Ref: (a) NAVAUDSVC ltr 7510/2013-064, dated 16 Apr 13
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

Encl: (1) Status of Recommendations
(2) Background and Pertinent Guidance
(3) Scope and Methodology
(4) Statistical Sampling Methodology and Detailed Projections
(5) Activities Visited and/or Contacted
(6) Management Response from Deputy, Chief of Naval Personnel

1. Introduction.

a. We have completed the subject audit announced in reference (a), and are providing the audit report in accordance with reference (b). We found that the Bureau of Naval Personnel (BUPERS) could not identify all users, as required, who could and did access the Mechanicsburg Mainframe Systems. Additionally, the System Authorization Access Request-Navy (SAAR-N) forms provided by BUPERS were incomplete. For details, please see paragraph 5 for Audit Results. Paragraph 7 provides our recommendations to the Deputy, Chief of Naval Personnel (CNP), as well as management responses and our comments on the responses. Enclosure 1 provides the status of the recommendations.

b. Actions taken by the Deputy, Chief of Naval Personnel meet the intent of Recommendations 3 and 4, and those recommendations are closed. Actions planned by the Deputy, Chief of Naval Personnel meet the intent of Recommendations 1 and 2. These recommendations are considered open pending completion of the planned corrective actions, and are subject to monitoring in accordance with reference (b). Management should provide a written status report on the open recommendations within 30 days after target completion dates.

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA**
(AUDIT REPORT N2015-0026)

2. Reason for Audit and Objective.

a. The former Deputy, CNP/Commander, Navy Personnel Command (NPC) requested an audit of the management of Navy corporate data¹ on the Mechanicsburg, PA Mainframe following a breach of personally identifiable information at NPC.

b. The audit objective was to determine if management controls over Navy corporate data on the mainframe located in Mechanicsburg, PA were in place and operating as intended to protect the information from unauthorized disclosure.

3. Background.

a. Navy corporate data resides on various systems on numerous mainframes located throughout the United States. On the Mechanicsburg, PA Mainframe, there are four BUPERS systems that are referred to in this report as the Mechanicsburg Mainframe Systems. These systems contain personnel data with highly sensitive personally identifiable information. Additionally, the mainframe data stores and provides numerous data feeds to other systems across the Navy enterprise.

b. The Mechanicsburg Mainframe is maintained by the Defense Information Systems Agency (DISA). Space and Naval Warfare (SPAWAR) Systems Center (SSC) Atlantic, New Orleans, LA is responsible for the technical management of the Mechanicsburg Mainframe Systems. BUPERS is responsible for managing account access. NPC operates the Personnel Systems (PERS), the Navy Manpower and Personnel Distribution System (NMPDS), and the Inactive Manpower and Personnel Management Information System (IMAPMIS). Navy Manpower Analysis Center (NAVMAC) operates the Total Force Manpower Management System (TFMMS). CNP has overall responsibility for BUPERS, NPC, and NAVMAC.

c. To gain access to a Navy Information Technology (IT) system, an individual must complete a SAAR-N form as required by the All Commands (ALCOM) 170/11, Navy Telecommunications Directive, "SAAR-N." An individual's access is contingent on the information provided on the SAAR-N form: having a need-to-know, completion of the annual information assurance (IA) training, and at least the minimum required security clearance. The form is to be signed by the user, the supervisor, the IA manager, the security manager, and the information owner prior to receiving access to the system being requested. BUPERS receives the SAAR-N forms internally or from other commands to approve access to the Mechanicsburg Mainframe Systems. Then, the account is activated

¹ As used in this report, the term Navy corporate data refers to the Personnel Systems (PERS), the Navy Manpower and Personnel Distribution System (NMPDS), the Inactive Manpower and Personnel Management Information System (IMAPMIS), and the Total Force Manpower Management System (TFMMS).

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

either by BUPERS or by SPAWAR, depending on the system (see Enclosure 2 for detailed background information).

4. Scope and Methodology.

a. Our audit scope consisted of the four BUPERS systems on the Mechanicsburg Mainframe Systems. They are:

- PERS (Personnel Systems);
- NMPDS (Navy Manpower and Personnel Distribution System);
- IMAPMIS (Inactive Manpower and Personnel Management Information System);
and
- TFMMS (Total Force Manpower Management System).

b. We conducted interviews to determine procedures and practices regarding access to the Mechanicsburg Mainframe Systems. We requested key BUPERS and SSC Atlantic personnel provide a list of the approved users who could access the Mechanicsburg Mainframe Systems from 1 January 2012 through 31 March 2013. SSC Atlantic provided a list of 4,810² unique users who accessed the systems from December 2011 through April 2013. We selected a weighted statistical sample³ from two distinct categories: (1) 150 user identification numbers with user names, and (2) 150 user identification numbers only for a total sample of 300 user⁴ identification numbers. For statistical sampling details, please see Enclosure 4.

c. We requested SAAR-N forms for the 300 sampled users from key BUPERS personnel. However, we only received and verified 347 SAAR-N forms for 237 users correlated with our sample. There were multiple forms for some users. We reviewed key information on the SAAR-N forms and the SAAR-N Addendum⁵ in order to determine their completeness: correct system(s) accessed, required approval signatures, IA training information, access expiration dates, need-to-know information, and proper security information. For more details on our scope and methodology, please see Enclosure 3.

² The total universe consists of 2,362 user names and 2,448 user identification numbers with blanks in the name field.

³ A sample weighted on the number of applications was designed so that the probability of selecting any given user equals the number of applications that user had accessed. For example, a user who had accessed two applications would have twice the probability of being selected than a user who had accessed one application.

⁴ Due to the weighted design, some of the users were selected more than once.

⁵ The SAAR-N addendum is an additional form used for access to Mechanicsburg Mainframe Systems.

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

5. **Audit Results.** BUPERS could not identify all users, as required, who could and did access the Mechanicsburg Mainframe Systems. Additionally, the SAAR-N forms provided by BUPERS were incomplete. This occurred because BUPERS' access management controls were insufficient and not operating as required to protect information from unauthorized disclosure. Also, BUPERS did not follow already established access control guidance on granting and monitoring access to the Mechanicsburg Mainframe Systems, to include completion of the SAAR-N forms. As a result, there was (and unless corrected, still is) a risk of unauthorized users accessing Navy IT systems, which made BUPERS vulnerable to the inappropriate release of sensitive and/or personally identifiable information.

a. **Established Access Controls.**

(1) Access controls protect data and information systems by granting access to authorized users and denying access when the users do not have a need-to-know. Our analysis showed access control weaknesses that need to be improved. We found that BUPERS could not identify all users who could and did access the Mechanicsburg Mainframe Systems as required. Department of Defense (DoD) Instruction 8500.2 and Secretary of the Navy (SECNAV) Manual 5239.1 require a comprehensive account management process to ensure controls are in place for acceptance and monitoring of access.

(2) We could not obtain a complete list of all users who could access the Mechanicsburg Mainframe Systems. Even though some information owners provided lists of their system users, they did not contain all users for all the systems. In order to obtain a complete user list, we requested it from SSC Atlantic, which provided a list of 4,810 unique users who accessed the systems between December 2011 and April 2013. However, 2,448 of the 4,810 unique users provided did not contain the related user name.

(3) To gain access to Navy IT systems, the users are required to complete a SAAR-N form. When we asked that BUPERS personnel provide SAAR-N forms for the 300 users in our sample, we did not receive SAAR-N forms for 63 of the 300 users. We were told that some of the missing SAAR-N forms had been destroyed. Each information owner had a different response of how long a SAAR-N form is to be retained. However, BUPERS is required by the ALCOM 170/11, "Navy Telecommunications Directive, SAAR-N," to have a SAAR-N form for each system user. Also, the SECNAV Records Retention Manual 5210.1 requires that these forms be maintained for 6 years after account termination. Since BUPERS was unable to provide a complete list of users' identification numbers and related user names for those that could and did access the Mechanicsburg Mainframe Systems, we concluded they could not have monitored account access for all their systems as required by DoD Instruction 8500.2 and SECNAV Manual 5239.1. Also, since BUPERS was unable to provide all the SAAR-N forms for our sampled users, we concluded they could not have determined if

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

users were properly granted access to their systems to prevent unauthorized disclosure, as required by ALCOM 170/11 and the SECNAV Records Retention Manual 5210.1.

b. SAAR-N Forms.

(1) Our review of the 347 SAAR-N forms for 237 users found that a significant number of the forms did not comply with ALCOM 170/11 for the following reasons:

- 147 of the 237 users' SAAR-N forms or SAAR-N Addendums did not request the system(s) which they accessed, including one classified system.⁶ *We estimated that of the 4,810 users, approximately 2,120 users accessed system(s) that were not requested on their SAAR-N forms or SAAR-N Addendums.*⁷
- 279 of the 347 forms were missing all of the SAAR-N form's Part IV (system account information),⁸ while the remaining 68 forms were only partially completed. *We estimated that of the 7,531 SAAR-N forms, 4,076 forms were missing Part IV.*
- 176 of the 347 forms were missing at least 1 of the 5 required signatures.⁹ Specifically, 144 forms were missing 1 signature, 31 forms were missing 2 signatures, and 1 was missing 3 signatures. *We estimated that of the 7,531 SAAR-N forms, 2,716 SAAR-N forms were missing at least 1 signature.*
- 39 of the 347 forms did not indicate required IA training completion. Additionally, 20 of the 347 forms indicated that the user completed training; however, it was not within a year of signing the form as required by the ALCOM 170/11. Of the 347 forms, 53 were undetermined because there were no user signature dates on the form to determine the time between IA training and access request. *We estimated that of the 7,531 SAAR-N forms, 498 SAAR-N forms did not indicate completion of IA Training.*
- 67 of the 347 forms did not indicate a user's need-to-know; however, DoD Instruction 8500.2 requires IA officers to ensure all users have a need-to-know. *We estimated that of the 7,531 SAAR-N forms, 1,020 SAAR-N forms did not indicate a user's need-to-know.* Also, 64 of the 240¹⁰ forms for military/contractor personnel did not contain a projected rotation date/contract expiration date that would indicate when they no longer had a need-to-know.

⁶ TFMMS.

⁷ We are 95 percent confident that the number of users who accessed systems not requested on their SAAR-N forms is between 1,834 and 2,415 users.

⁸ Part IV on the SAAR-N form is to be completed by authorized staff identifying the system(s) account code, the server, the applications the user has been approved for, and when it was processed.

⁹ The five required signatures on a SAAR-N form are from the following: the user, the supervisor, the information owner, the IA manager, and the security manager.

¹⁰ Civilians were not included in this analysis since they do not have a projected rotation or expiration date.

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

We estimated that of the 7,531 SAAR-N forms, 744 forms did not contain a projected rotation date/contract expiration date.

- 14 of the 347 forms indicated that system access was approved without the minimum background investigations of a National Agency Check with Law and Credit (NACLC) as required by SECNAV Manual 5510.30. Specifically, 7 of the 14 forms indicated that the user had a National Agency Check with Inquiries (NACI), which is below the minimum requirement for access. Additionally, 7 of the 14 forms were undetermined because the page was missing, or it did not indicate which investigation was conducted. *We estimated that of the 7,531 SAAR-N forms, 181 SAAR-N forms indicated that system access was approved without the minimum background investigations of an NACLC.*
- 35 of the 347 forms were not marked with the appropriate IT level¹¹ by the security manager for system access. SECNAV Manual 5510.30 requires that a Level I or II IT level designation be received and maintained prior to being granted access to privileged and/or sensitive information within Navy IT systems. *We estimated that of the 7,531 SAAR-N forms, 473 forms were not marked with the appropriate IT level.*
- 19 of 158 forms¹² investigation dates did not match the investigation dates in the Joint Personnel Adjudication System (JPAS), and 9 of the 158 forms' types of investigations did not match JPAS records. We also identified one user who had access for 16 months with a NACI investigation, which is below the minimum requirement for access. Another user was granted access with a revoked clearance and had that access for the next 17 months. BUPERS terminated both users' access when Naval Audit Service team members notified the information owners on 2 June 2014. *We estimated that of the 7,531 SAAR-N forms, 326 forms' investigation dates did not match with JPAS and 131 forms' type of investigation did not match with JPAS.*

For full detailed statistical projections of the SAAR-N form completeness results, see Enclosure 4.

(2) BUPERS's SAAR-N forms were incomplete because BUPERS was not following already established access control guidance, and there was no standard written process for how the SAAR-N forms were to be fully completed and approved. Each key

¹¹ IT Level I users must have a Single Scope Background Investigation (SSBI) or SSBI-Periodic Reinvestigation, which allows access to Sensitive Compartmented Information (SCI) or Top Secret information. IT Level II users must have an NACLC, which allows access to sensitive information. IT Level III does not allow access to sensitive information and therefore, they are not allowed access to the Mechanicsburg Mainframe Systems.

¹² Neither the Social Security number (SSN), nor the DoD Electronic Data Interchange Person Identifier (DoD EDI PI) fields are required to be completed on the SAAR-N form. However, since 158 of the 347 forms contained this information, we were able to use it to access the user's security clearance in JPAS to determine if their background information was the same as that reported on the SAAR-N form.

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

player had a different SAAR-N completion and approval process. Many SAAR-N forms were submitted from commands outside of BUPERS and BUPERS did not review all the forms prior to granting access. SAAR-N forms originating within BUPERS were routed through the BUPERS and NPC security manager and either the BUPERS or NPC IA manager for review prior to access approval. Additionally, the BUPERS IA Office verifies that users had completed IA training within the past year prior to granting access. The NPC IA Office does not verify IA training. Instead, the NPC IA Office awaits notifications that a user is due for annual IA training.

(3) Without proper access controls in place, the potential exists for unauthorized users to continue to access the Mechanicsburg Mainframe Systems, and for users to continue to receive access to the systems without having the proper security clearance and IT levels. This leaves BUPERS vulnerable to the inappropriate release of sensitive and/or personally identifiable information.

6. Briefings with Management. We provided preliminary results to the Deputy, Chief of Naval Personnel on 29 April 2015. Additionally, we provided status briefs to BUPERS personnel throughout our audit to include a preliminary results brief on 22 July 2014.

7. Recommendations and Corrective Actions. Deputy, Chief of Naval personnel provided management responses to the recommendations. The responses and our comments follow. The full text of the management's response is in Enclosure 6.

We recommend that the Deputy, Chief of Naval Personnel:

Recommendation 1. Develop and implement controls to ensure only authorized users can access the Mechanicsburg Mainframe Systems as required by Department of Defense Instruction 8500.2 and Secretary of the Navy Manual 5239.1.

Management response to Recommendation 1. Concur. The Office of the Deputy, Chief of Naval Personnel is drafting a Bureau of Personnel (BUPERS) Instruction (BUPERS Instruction 5239 series) to provide specific guidelines for the correct completion of the mandatory System Authorization Access Request – Navy (SAAR-N) in accordance with the Secretary of the Navy Manual 5239.1 and the All Commands (ALCOM) 170/11. The SAAR-N standard operating procedures (SOP) will be included in the BUPERS Instruction 5239. An addendum has been added to the SAAR-N to further limit users' access to detailing community.

Naval Audit Service comment on the response to Recommendation 1. Actions planned meet the intent of the recommendation. In subsequent communication, the Office of the Deputy, Chief of Naval Personnel stated that the BUPERS Instruction would specifically address the proper

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

processing of the information owner's signature section on the SAAR-N form and the completion of the SAAR-N form's Part IV (list of systems a member is being granted access) when access is being granted. The estimated completion date is 23 October 2015. The recommendation will be open until the BUPERS Instruction 5239 is issued and provides specific guidelines for the correct completion of the SAAR-N form.

Recommendation 2. Implement controls to ensure the System Authorization Access Request-Navy form is fully completed in accordance with the All Commands 170/11, "Navy Telecommunications Directive, System Authorization Access Request-Navy."

Management response to Recommendation 2. Concur. The Office of the Deputy, Chief of Naval Personnel has drafted an internal standard operating procedure (SOP) (BUPERS-07301) to provide users, supervisors, information owners, security personnel and Information System Security Managers with specific guidelines for the correct completion, storage and retention of the mandatory SAAR-N in accordance with ALCOM 170/11.

Naval Audit Service comment on the response to Recommendation 2. Actions planned meet the intent of the recommendation. In subsequent communication, the Office of the Deputy, Chief of Naval Personnel stated that they are using the SAAR-N form as their internal control to ensure only authorized users can access the systems. The estimated completion date is 30 October 2015. The recommendation 2 will be open until the internal SOP is issued and provides specific guidelines for the correct completion, storage, and retention of the mandatory SAAR-N form.

Recommendation 3. Develop and implement controls to ensure users have the minimum National Agency Check with Law and Credit background investigation and are granted the correct information technology level of system access prior to receiving access as required by Secretary of the Navy Manual 5510.30.

Management response to Recommendation 3. Concur. All positions within BUPERS and Navy Personnel Command have been designated non-critical sensitive or higher and require a National Agency Check with Law and Credit (NACLC) for hire as a condition for employment. The date of the investigation reported on the SAAR-N form is the investigation closed date. Reinvestigation is initialed based upon the security clearance tracker date.

Naval Audit Service comment on the response to Recommendation 3. Actions taken meet the intent of the recommendation. In subsequent communication, the Office of the Deputy, Chief of Naval Personnel stated that a new Navy Personnel Command Information Assurance team member began taking steps in May 2015 to ensure that all SAAR-N forms from

FOR OFFICIAL USE ONLY

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

external customers are properly validated and filled in by utilizing ongoing Navy Reserve personnel support. Also, the security manager now validates the background investigation or clearance information of those requesting Level 1 or Level 2 access. Action was completed on 31 May 2015 and the recommendation is closed.

Recommendation 4. Retain the System Authorization Access Request-Navy forms for 6 years in accordance with Secretary of the Navy Manual 5210.1.

Management response to Recommendation 4. Concur. The Office of the Deputy, Chief of Naval Personnel has drafted an internal SOP (BUPERS-07301) updating the SAAR-N form process in accordance with governing policy to include annual reviews and the requirement to retain for 6 years.

Naval Audit Service comment on the response to Recommendation 4. Actions taken meet the intent of the recommendation. In subsequent communication, the Office of the Deputy, Chief of Naval Personnel stated that the command commenced retaining the SAAR-N forms for 6 years in May 2015. Action was completed on 31 May 2015 and the recommendation is closed.

8. Other Information.

a. Please provide all correspondence to the Assistant Auditor General for Manpower and Reserve Affairs Audits, XXXXXXXXXXXXXXXX, by email at XXXXXXXXXXXXXXXXXXXX, with copies to the Director, Policy and Oversight, XXXXXXXXXXXXXXXXXXXX, and the Naval Audit Service Follow-up Coordinator, XXXXXXXXXXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)
FOIA (b)(6)
FOIA (b)(6)

b. In order to protect privacy and other sensitive information included in this report, we request that you do not release this report outside the Department of the Navy, post on non-Naval Audit Service Web sites, or in Navy Taskers without the prior approval of the Auditor General of the Navy.

FOR OFFICIAL USE ONLY

Subj: **MANAGEMENT CONTROLS OF NAVY CORPORATE DATA
(AUDIT REPORT N2015-0026)**

c. We appreciate the cooperation and courtesies extended to our auditors.



FOIA (b)(6)

XXXXXXXXXXXXXXXXXXXX

Assistant Auditor General
Manpower and Reserve Affairs Audits

Copy to:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAVRDA
CNO (VCNO, DNS-33, N40, N41)
CMC (ACMC)
CNP
DON CIO
SPAWAR
NAVINSGEN (NAVIG-14)
AFAA/DO

Enclosure 1:

Status of Recommendations

Recommendations							
Finding ¹³	Rec. No.	Page No.	Subject	Status ¹⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ¹⁵
1	1	7	Develop and implement controls to ensure only authorized users can access the Mechanicsburg Mainframe Systems as required by Department of Defense Instruction 8500.2 and Secretary of the Navy Manual 5239.1.	O	Deputy, Chief of Naval Personnel	10/23/2015	
1	2	8	Implement controls to ensure the System Authorization Access Request-Navy form is fully completed in accordance with the All Commands 170/11, "Navy Telecommunications Directive, System Authorization Access Request-Navy."	O	Deputy, Chief of Naval Personnel	10/30/2015	
1	3	8	Develop and implement controls to ensure users have the minimum National Agency Check with Law and Credit background investigation and are granted the correct information technology level of system access prior to receiving access as required by Secretary of the Navy Manual 5510.30	C	Deputy, Chief of Naval Personnel	5/31/2015	
1	4	9	Retain the System Authorization Access Request-Navy forms for 6 years in accordance with Secretary of the Navy Manual 5210.1.	C	Deputy, Chief of Naval Personnel	5/31/2015	

¹³ / + = Indicates repeat finding.

¹⁴ / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed;

U = Recommendation is undecided with resolution efforts in progress.

¹⁵ If applicable.

Background and Pertinent Guidance

Background

The Bureau of Naval Personnel (BUPERS) uses four systems on the Mechanicsburg, PA Mainframe, and those systems are hereafter referred to as Mechanicsburg Mainframe Systems. The systems contain highly sensitive personally identifiable information, as well as one classified system, the Total Force Manpower Management System (TFMMS). Additionally, they store data and provide numerous data feeds to other personnel systems that affect systems and functions in the Fleet across the Navy enterprise. Navy Personnel Command information owners oversee the functionality and data contained on the Personnel Systems, the Navy Manpower and Personnel Distribution System, and the Inactive Manpower and Personnel Management Information System, while a Navy Manpower Analysis Center (NAVMAC) information owner oversees the functionality and data of TFMMS. Both NAVMAC and Navy Personnel Command are owned by BUPERS, who is responsible for managing account access to their Mechanicsburg Mainframe Systems.

The Mechanicsburg Mainframe Systems are maintained by the Defense Information Systems Agency. This agency provides the network, computing infrastructure, and enterprise services to support information sharing and decision making for the systems. All access to the Mechanicsburg Mainframe Systems is controlled through the Defense Information Systems Agency's firewalls, which exclude users without approved common access cards or approved Internet protocols.

The Mechanicsburg Mainframe Systems are included in the Budget Submitting Office 39 systems and are managed by Program Manager; Warfare (PMW)-240 which is the Navy's Sea Warrior Program and is a part of the Navy Program Executive Office for Enterprise Information Systems. Space and Naval Warfare (SPAWAR) Systems Center (SSC) Atlantic, New Orleans, LA is responsible for the administration of the production processing environment of the Mechanicsburg Mainframe Systems. SSC Atlantic assists PMW-240 with providing cradle-to-grave management of the acquisition, deployment, sustainment, and retirement of roughly one third of the systems in the manpower, personnel, training and education domain to include the Mechanicsburg Mainframe Systems.

Pertinent Guidance

Department of Defense (DoD) Instruction 8500.2, “Information Assurance (IA) Implementation,” dated 6 February 2003, requires a comprehensive account management process to be implemented to ensure that only authorized users can gain access to workstations, applications, and networks, and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. Additionally, it ensures that information ownership responsibilities are established for each DoD information system, to include accountability, access approvals, and special handling requirements. The instruction requires initial and periodic refresher IA training for all DoD employees. IA roles and responsibilities at all organizational and information technology (IT) levels shall be clearly delineated in policy and doctrine. Each IA officer shall assist the IA manager and ensure that all users have the requisite security clearances and supervisory need-to-know authorization, and are aware of their IA responsibilities before being granted access to DoD information systems.

Secretary of the Navy (SECNAV) IA Manual 5239.1, “Department of the Navy (DON) IA Program,” dated November 2005, states the DON Chief Information Officer is responsible for developing and promulgating IA strategy and policy, coordinating IA within the department and with other DoD components, measuring and evaluating service and system-level IA performance, and reporting to SECNAV on the effectiveness of DON IA activities. Information and information systems shall be properly managed and protected as required by law, regulation, policy, or treaty. The IA manager is responsible to the local IA command authority and designated approval authorities for ensuring the security of an IT system, and that it is approved, operated, and maintained throughout its life cycle in accordance with IT system security certification and accreditation documentation. All DON information systems and networks shall include written standard operating procedures, which are routinely updated and tailored to reflect changes in the operational environment. An individual’s access to DON information and resources is contingent upon having the need-to-know, holding the appropriate security clearances, and authorization by the cognizant DON commanding officer. Initial IA awareness training shall be provided to all military, civilian, and contractor personnel as a condition of access to DON information systems in any system life cycle phase. System administrators shall monitor user account inactivity and establish procedures for investigating, deactivating, and eliminating accounts that do not show activity over time.

SECNAV Records Retention Manual 5210.1, dated January 2012, requires that inactive user identifications, profiles, authorizations and password files should be destroyed or deleted 6 years after a user account is terminated, password is altered, or when no longer needed for investigative or security purposes, whichever is later.

SECNAV DON Personnel Security Program Manual 5510.3, dated June 2006, states that a user must have a minimum of a National Agency Check with Law and Credit prior to receiving access to Confidential and Secret classified national security information. The basis requirement for assignment for IT-II and IT-III positions is the National Agency Check with Law and Credit.

All Commands 170/11, “Navy Telecommunications Directive, System Authorization Access Request - Navy (SAAR-N),” dated October 2011, announces the implementation of the Office of the Chief of Naval Operations form 5239/14 (Rev. 9/2011), SAAR-N form. All users requiring access to Navy IT resources must sign a SAAR-N form. Users shall complete DoD annual IA awareness training prior to signing a SAAR-N form. The completed forms shall be retained by the command IA manager and/or security manager.

Scope and Methodology

Scope

We conducted this audit from 16 April 2013 to 19 May 2015. The conditions noted existed for the Mechanicsburg, PA Mainframe Systems for users who had accessed the systems from December 2011 through April 2013.

The audit focused on 26 applications among 4 Bureau of Naval Personnel (BUPERS) systems on the Mechanicsburg Mainframe: Personnel Systems, Navy Manpower and Personnel Distribution Systems, Inactive Manpower and Personnel Management Information System, and Total Force Manpower Management System (TFMMS). They are referred to throughout the report as the Mechanicsburg Mainframe Systems.

We obtained a list of user identification numbers and related user names of who had accessed the Mechanicsburg Mainframe Systems from Space and Naval Warfare (SPAWAR) Systems Center (SSC) Atlantic, which resulted in a universe of 689,289 records for individuals who had accessed the systems from December 2011 through April 2013. We used SSC Atlantic's list because not all the BUPERS information owners were able to provide a list of users for our timeframe. From the SSC Atlantic records, we identified a universe of 4,810 unique users. The universe of 4,810 users was associated with 7,531 System Authorization Access Request-Navy (SAAR-N) forms. We then identified 2,362 user names and 2,448 user identification numbers with no related user name.

Methodology

To accomplish this audit, we researched and reviewed applicable Federal, Department of Defense (DoD), and Department of the Navy laws, regulations, and directives. We evaluated compliance with existing guidance and assessed internal controls related to the Mechanicsburg Mainframe Systems. We made inquiries and held discussions with key personnel at the commands and activities listed in Enclosure 5. We determined the key officials' roles and responsibilities as they pertained to the Mechanicsburg Mainframe Systems. We did not identify any prior Government Accountability Office, DoD Inspector General, or Naval Audit Service audit reports relating to management controls of Navy corporate data; therefore, no follow up was required.

We requested a list of authorized users who could access the Mechanicsburg Mainframe Systems from 1 January 2012 through 31 March 2013 from the systems' information owners, BUPERS and Navy Personnel Command (NPC) information assurance managers, the BUPERS and NPC security manager, and the systems' technical managers at SSC Atlantic.

SSC Atlantic provided a list of users who accessed the Mechanicsburg Mainframe Systems from December 2011 through April 2013. We used the SSC Atlantic list to create our two samples since they were able to provide a list of users who accessed the Mechanicsburg Mainframe Systems within our timeframe. SSC Atlantic provided a list of 4,810¹⁶ unique users who had accessed the systems from December 2011 through April 2013. The 4,810 users had a potential universe total of 7,531 SAAR-N forms. We selected a weighted sample from two distinct categories: (1) 150 user identification numbers with user names, and (2) 150 user identification numbers only for a total sample of 300 user identification numbers. These 300 users had the potential of a total of 532 SAAR-N forms. See Enclosure 4 for detailed sampling methodology.

We requested that key personnel provide the SAAR-N forms for the 300 users identified in both of our samples. We received 357 SAAR-N forms for 246 user identification numbers. We then asked that they provide documentation to verify that the SAAR-N forms provided for these individuals correctly corresponded to the user identification number and name in our sample. From the key players, we received an Accessed Control Facility document generated by the mainframe, a Time Sharing Option Tracker spreadsheet, a TFMMS Action Officer Report used to track the activation and deactivation of TFMMS accounts, and a spreadsheet of active and deleted Officer Personnel Information System users. Following the receipt of this documentation, we verified that there were 237 users¹⁷ and 347 forms.

For these 237 users, we received 347 forms since some users had multiple SAAR-N forms, to include DoD SAAR forms. We documented key information off of the SAAR-N forms in order to perform a detailed analysis for the completeness and accuracy of the forms. Specifically, we determined if: the system(s) listed on the SAAR-N form and SAAR-N Addendum matched the system(s) that the user accessed during our timeframe according to the SSC Atlantic list; all five required signatures were on the form; users had a need-to-know indicated on their form; military and contractor personnel indicated access expiration dates on their form; and forms included account information. We compared the date the user signed the form with the information assurance training date on the user's form.

¹⁶ The total universe consists of 2,362 user names and 2,448 user identification numbers with blanks in the name field.

¹⁷ Nine users and their 10 related forms were removed from our analysis because BUPERS was unable to provide verification documents.

Using the user's Social Security number and/or DoD Electronic Data Interchange Person Identifier that was on the SAAR-N forms, we obtained Joint Personnel Adjudication System (JPAS) security information for each user. Then, we compared the JPAS information of a user with part III of the SAAR-N form to ensure the security manager validated security information on the form. Additionally, for all 347 forms obtained, we identified if the form indicated that the user had at least a National Agency Check with Law and Credit investigation prior to being granted access to the systems and that the form indicated the user had a Level I or II IT level.

We conducted this 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. We also assessed the reliability of SSC Atlantic's list of users by verifying the user IDs to the provided SAAR-N forms, and we determined that the data was sufficiently reliable for the purpose of this audit.

The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. During this audit, we identified internal control weaknesses in the management of Navy corporate data on the Mechanicsburg, PA mainframe. In our professional judgment, the control weaknesses may warrant reporting in the Auditor General's annual Federal Managers' Financial Integrity Act memorandum identifying management control weaknesses to the Secretary of the Navy.

Enclosure 4:

Statistical Sampling Methodology and Detailed Projections

Statistical Sampling Methodology

Space and Naval Warfare Systems Center (SSC) Atlantic provided a list of 4,810¹⁸ unique users who accessed the systems from December 2011 through April 2013. The 4,810 users had a potential universe total of 7,531 System Authorization Access Request-Navy (SAAR-N) forms. We selected a sample, using a weighted sampling design, from SSC Atlantic's list of users who accessed the Mechanicsburg Mainframe Systems. The sampling weight used to pull the samples was based on the number of distinct applications a user accessed within the provided list. A sample weighted on the number of applications is designed so that the probability of selecting any given user equals the number of applications that user has accessed. For example, a user who has accessed two applications would have twice the probability of being selected than a user who has accessed one application. Since one application represented one potential SAAR-N form, this type of weighting should increase the efficiency of the sample design when projecting to SAAR-N forms within the universe of forms. We selected a statistical sample of 150 user identification numbers with user names and 150 user identification numbers without names.

The sample size was selected to give sufficient precision, at a 95-percent confidence level, for projections associated with system access. Due to the weighted design, both sample lists were selected with replacements to reduce bias when estimating the point estimates and confidence intervals. This means some of the users were selected more than once. The 300 users selected in the sample had the potential of 532 forms. Each individual could have accessed anywhere from one application to a maximum of five applications. As a result of the sample weights, there were 169 users selected in the sample that had accessed more than one application.

¹⁸ The total universe consists of 2,362 user names and 2,448 user identification numbers with blanks in the name field.

Statistical Sampling Projection Results

Based on the universe of 7,531 SAAR-N forms and the results of our SAAR-N form weighted sample review, our statistical sampling projected results are found in the following table.

Table 1. Statistical Sampling Projection Results

<i>Identified Issues on SAAR-N Form</i>	<i>95% Lower Bound</i>	<i>Point Estimate</i>	<i>95% Upper Bound</i>
Missing Part IV ¹⁹	3,722 74%	4,076 80%	4,424 84%
Missing at least one signature	2,380 47%	2,716 53%	3,070 59%
Did not complete information assurance (IA) training	355 7%	498 10%	693 13%
Did not complete IA training within a year	180 4%	289 7%	460 10%
Undetermined if completed IA training	528 10%	703 14%	927 18%
Did not indicate need-to-know	794 16%	1,020 20%	1,299 25%
No projected rotation date/expiration date ²⁰	570 18%	744 23%	963 29%
No minimum background investigation	101 2%	181 4%	324 6%
No appropriate Information Technology level	331 6%	473 9%	670 13%
Form investigation date did not match Joint Personnel Adjudication System	202 9%	326 14%	521 22%
Form investigation type did not match Joint Personnel Adjudication System	62 3%	131 6%	271 11%

¹⁹Part IV on the SAAR-N form is to be completed by authorized staff identifying the system(s) account code, the server, the applications the user has been approved for, and when it was processed.

²⁰ Civilians were not included in this analysis, since they do not have a projected rotation or expiration date.

Enclosure 5:

Activities Visited and/or Contacted

Defense Information Systems Agency, Mechanicsburg, PA

Chief of Naval Operations, Chief Information Office Division, Arlington, VA

United States Fleet Cyber Command, Network-Integration-Division, Norfolk, VA

Space and Naval Warfare Systems Program Manager Warfare-240, Program Executive Office for Enterprise Information Systems Sea Warrior Program, Alexandria, VA

Space and Naval Warfare Systems Center Atlantic, New Orleans, LA*

Bureau of Naval Personnel Office of Inspector General, Millington, TN*

Bureau of Naval Personnel Chief of Information Office, Millington, TN*

Bureau of Naval Personnel Information Assurance Management Office, Millington, TN*

Navy Manpower Analysis Center, Millington, TN*

Naval Personnel Command (PERS), Millington, TN*

 PERS-3: Personnel Information Management Department Branch

 PERS-31: Records Support Division

 PERS-32: Performance Evaluation Division

 PERS-33: Data Quality Maintenance Division

 PERS-45: Distribution Operations Management Branch

 PERS-534: Security Branch

 PERS-54: Information Technology Division

 PERS-802: Eligibility and Promotions Branch

 PERS-94: Functions Integrated Division

*Activities visited

Enclosure 6:

Management Response from Deputy, Chief of Naval Personnel



DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

7500
BUPERS-00B/340
June 19, 2015

From: Deputy Chief of Naval Personnel
To: Assistant Auditor General for Manpower and Reserve Affairs
Audits, Naval Audit Service
Subj: MANAGEMENT RESPONSE TO DRAFT AUDIT REPORT 2013-064, "MANAGEMENT
CONTROLS OF NAVY CORPORATE DATA" DATED 19 MAY 2015
Ref: (a) NAVAUDSVC memo 7510/2013-064 of 19 May 15 w/subject report
Encl: (1) Management Response to Subject Draft Report

1. As required by reference (a), enclosure (1) provides the management response to recommendations 1 through 4.

2. My Audit Liaison is [REDACTED] BUPERS-00IG32,
[REDACTED] e-mail: [REDACTED]

[REDACTED]

Copy to:
CHNAVPER (BUPERS-00IG)
BUPERS-07

FOIA (b)(6)

FOIA (b)(6)

NAVAUDSVC DRAFT AUDIT REPORT 2013-064, "MANAGEMENT CONTROLS OF NAVY CORPORATE DATA" DATED 19 MAY 2015

FINDING 1: There is a risk of unauthorized users accessing Navy IT systems, which makes the Bureau of Naval Personnel (BUPERS) vulnerable to the inappropriate release of sensitive and/or personally identifiable information.

RECOMMENDATION 1: That the Deputy, Chief of Naval Personnel develop and implement controls to ensure only authorized users can access the Mechanicsburg Mainframe Systems as required by Department of Defense Instruction 8500.2 and Secretary of the Navy Manual 5239.1.

MANAGEMENT RESPONSE: Concur. We are drafting a BUPERS instruction (BUPERSINST 5239 series) to provide specific guidelines for the correct completion of the mandatory System Authorization Access Request - Navy (SAAR-N) in accordance with SECNAV Manual 5239.1 and ALCOM 170/11. The SAAR-N standard operating procedures (SOP) will be included in the BUPERSINST 5239. An addendum has been added to SAAR-N to further limit users' access to detailing community. Estimated completion date is 30 October 2015.

RECOMMENDATION 2: That the Deputy, Chief of Naval Personnel implement controls to ensure the System Authorization Access Request-Navy form is fully completed in accordance with the All Commands 170/11, "Navy Telecommunications Directive, System Authorization Access Request-Navy."

MANAGEMENT RESPONSE: Concur. We have drafted an internal SOP (BUPERS-07301) to provide users, supervisors, information owners, security personnel and Information System Security Managers (ISSM) with specific guidelines for the correct completion, storage and retention of the mandatory OPNAV form 5239/14 SAAR-N in accordance with ALCOM 170/11. Estimated completion date is 30 October 2015.

RECOMMENDATION 3: That the Deputy, Chief of Naval Personnel develop and implement controls to ensure users have the minimum National Agency Check with Law and Credit background investigation and are granted the correct information technology level of system access prior to receiving access as required by Secretary of the Navy Manual 5510.30.

MANAGEMENT RESPONSE: Concur. All positions within BUPERS and Navy Personnel Command (NAVPERSCOM) have been designated non-critical sensitive or higher and require a National Agency Check with Law and Credit (NACLC) for hire as a condition for employment. The date of the investigation reported on the SAAR-N form is the Investigation closed date. Reinvestigation is initiated based upon the security clearance tracker date. Action completed 22 May 2015.

RECOMMENDATION 4: That the Deputy, Chief of Naval Personnel retain the System Authorization Access Request-Navy forms for 6 years in accordance with Secretary of the Navy Manual 5210.1.

MANAGEMENT RESPONSE: Concur. We have drafted an internal SOP (BUPERS-07301) updating the SAAR form process in accordance with governing policy to include annual reviews and the requirement to retain for 6 years. Estimated completion date is 30 October 2015.

Enclosure (1)

~~FOR OFFICIAL USE ONLY~~

Use this page as
BACK COVER
for printed copies
of this report

~~FOR OFFICIAL USE ONLY~~