Report No. DODIG-2018-096

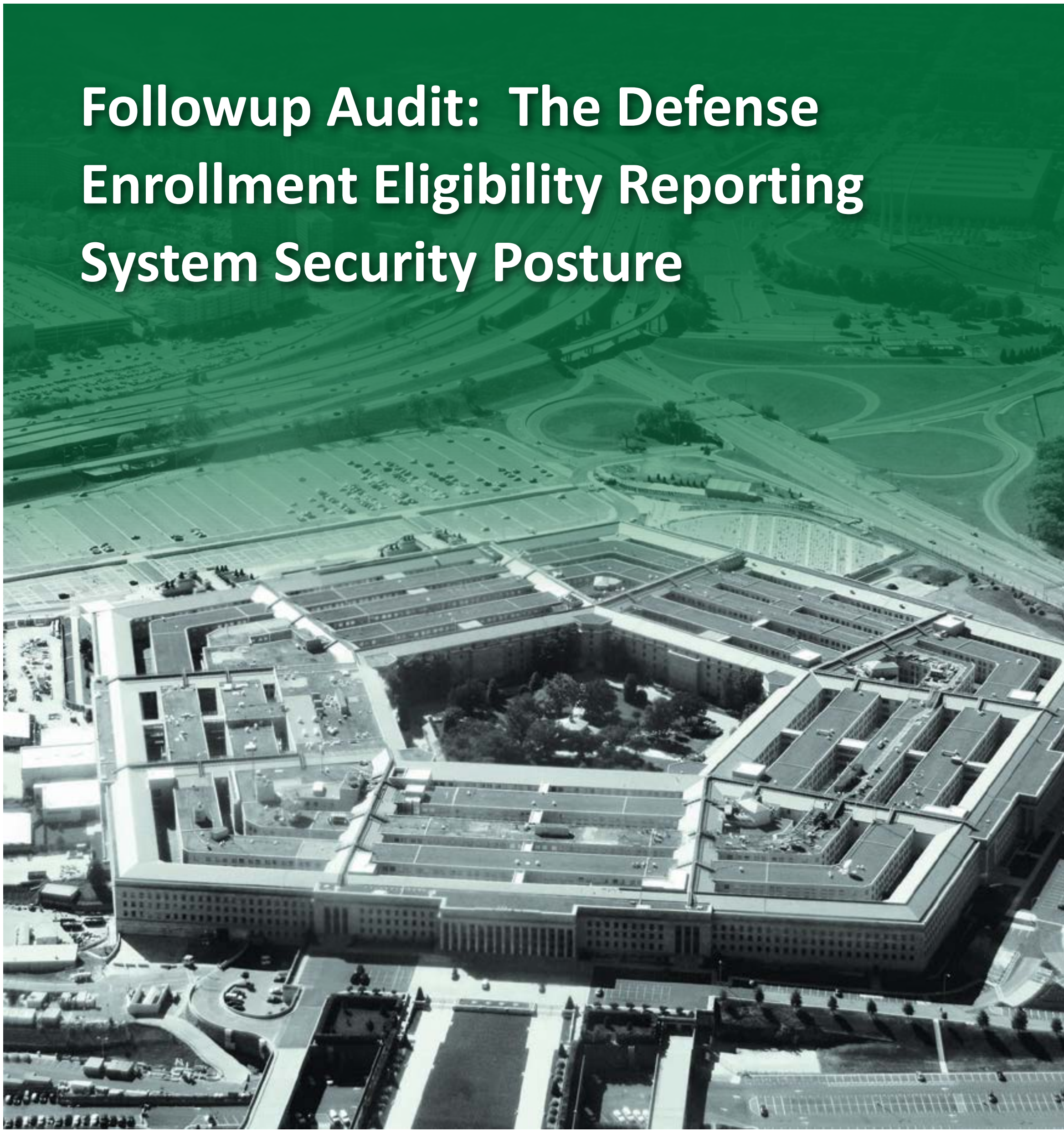
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

MARCH 30, 2018

Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline|800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture

March 30, 2018

Objective

We determined whether the Defense Manpower Data Center (DMDC) implemented corrective actions to remediate physical and cybersecurity weaknesses identified in Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012.

Background

The DMDC is a DoD field activity responsible for supporting the information management needs of the Office of the Under Secretary of Defense for Personnel and Readiness and reports to the Defense Human Resources Activity. The DMDC is responsible for managing, maintaining, and securing the Defense Enrollment Eligibility Reporting System (DEERS), which serves as a centralized DoD data repository containing personnel and medical data for Uniformed Service members, retirees, and their family members, DoD civilians' and DoD contractors.

DoD Office of Inspector General (DoD OIG) Report No. DODIG-2012-090 identified that DMDC management did not implement 33 cybersecurity controls for protecting DEERS from internal and external cyber threats. Specifically, 16 cybersecurity controls related to protecting DEERS security posture, 11 related to unauthorized access to DEERS, and 6 related to DEERS configuration management. The report contained 32 recommendations for DMDC officials to improve the DEERS security posture.

Findings

We determined that DMDC management implemented 28 of the 32 recommendations from Report No. DODIG-2012-090 and did not complete corrective actions for 4 recommendations. Specifically:

- ~~(FOUO)~~ the DMDC personnel did not apply the [redacted] because the DEERS servers have limited connectivity to the DoD Non-secure Internet Protocol Router Network;
- the DMDC Division Director relied on Employee Action Request Forms (EAFs) to out-process personnel and did not establish a centralized method;
- the DMDC Division Director EAF process did not include trusted agents for completing out-processing actions; and
- ~~(FOUO)~~ the DMDC Information System Security Officer did not implement a standard schedule for scans to verify and document the operational functionality of all [redacted]

Until DMDC increases their security posture, DEERS will continue to be vulnerable to increased cyberattacks that could jeopardize the integrity and confidentiality of sensitive DEERS data.

Recommendations

We recommend that the Director, DMDC:

- ~~(FOUO)~~ update [redacted] in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-53 requirements,
- establish a centralized procedure for out-processing terminated personnel,

Recommendations (cont'd)

- identify and appoint trusted agents responsible for out-processing personnel, and
- ~~(FOUO)~~ identify [redacted] [redacted] and establish a standardized scan schedule.

Management Comments and Our Response

During the audit, we notified the Director, DMDC, that corrective actions had not been completed for four of the recommendations from Report No. DODIG-2012-090. The Director initiated corrective actions during the follow-up audit to address the four recommendations. These recommendations from the original report are still open and we will close the recommendations once we verify that DMDC personnel have taken their agreed upon actions. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, Defense Manpower Data Center	N/A	1a, 1b, 1c, and 1d	N/A

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed-upon corrective actions were implemented.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 30, 2018

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY
DIRECTOR, DEFENSE MANPOWER DATA CENTER

SUBJECT: Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture (Report No. DODIG-2018-096)

We are providing this report for your information and use. We conducted this audit in accordance with generally accepted government auditing standards.

We did not issue a draft report, and no written response is required. During the audit, we notified the DMDC of our finding and recommendations. The DMDC management initiated actions during the audit to address the four recommendations. Therefore, we will close the recommendations once we verify that DMDC personnel have completed actions to address each recommendation.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Introduction

Finding. DMDC Improved DEERS Cybersecurity Controls But Additional Action Was Needed ... 4

Appendixes

Acronyms and Abbreviations ... 28

Introduction

Objective

We determined whether the Defense Manpower Data Center (DMDC) implemented corrective actions to remediate physical and cybersecurity weaknesses identified in Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture", May 22, 2012. See Appendix A for our scope and methodology and prior coverage related to the audit objective.

Background

The DMDC is a DoD field activity that is subordinate to the Defense Human Resources Activity and is responsible for supporting the information management needs of the Office of the Under Secretary of Defense for Personnel and Readiness. The DMDC is responsible for managing, maintaining, and securing the Defense Enrollment Eligibility Reporting System (DEERS), which is one of its largest operational programs. DEERS is a centralized DoD data repository containing personnel and medical data, including detailed personnel eligibility information for benefits and entitlements distributed to approximately 47 million Uniformed Service members, retirees, and their family members; DoD civilians; and DoD contractors.

The DEERS Program Management Office is located in Seaside, California (DMDC Seaside). DMDC Seaside manages the functionality and security posture of DEERS and serves as the DEERS alternate processing site in the event of a contingency.[1] The DMDC is responsible for the overall DEERS operating environment, including hardware and software configuration, and data integrity.

The DMDC Cybersecurity Division is responsible for designing and implementing cybersecurity controls to provide an integrated, layered protection for DEERS. The DMDC Cybersecurity Policy states that the Information System Security Manager is responsible for developing and maintaining an organizational or system-level cybersecurity program that includes cybersecurity architecture, and cybersecurity processes and procedures.

[1] Security posture is the security status of an enterprise's networks, information, and systems based on cybersecurity resources and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

2012 DEERS Audit Report Summary

In May 2012, the DoD Office of Inspector General (DoD OIG) issued Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012, addressing DEERS cybersecurity control weaknesses.[2] The objective was to evaluate whether controls were designed and effectively implemented over DEERS to deter and protect sensitive data from compromise by internal and external cyber threats. The DOD OIG determined that management did not implement 33 cybersecurity controls for protecting DEERS data from compromise by internal and external cyber threats. Of the 33 cybersecurity controls, 16 related to protecting the security posture, 11 related to preventing unauthorized access, and 6 related to configuration management processes.

Security Posture Improvements Needed

~~(FOUO)~~ In the report, the DOD OIG identified that DMDC Systems and Technical Support Division personnel did not fully protect the DEERS operating system [redacted].[3] In addition, DEERS Division and the DMDC Information Systems Security Group personnel did not maintain documentation supporting critical decisions affecting the DEERS security posture because they assessed risk using an unstructured, informal process.

Stronger Controls Needed to Prevent Unauthorized Access

In the report, the DoD OIG identified that DMDC personnel did not develop and implement appropriate procedures to account for personnel supporting DEERS operations, including those who perform cybersecurity responsibilities, because personnel from the:

- DEERS Division did not maintain current access control lists or verify whether five application managers responsible for managing access to DEERS applications at 45 sites maintained appropriate and accurate documentation and deactivated inactive accounts;
- DMDC Information Systems Security Group misinterpreted DoD policy and did not maintain sufficient documentation to support employee out-processing actions for 12 personnel;

[2] Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012.

[3] The DoD adopted the term "cybersecurity" defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 instead of "information assurance (IA)."

- DEERS and Systems Divisions did not periodically revalidate access; and
- Systems Division did not appropriately configure 8 of the 203 contractor e-mail accounts.

Weaknesses Existed in DEERS Configuration Management Practices

~~(FOUO)~~ In the report, the DOD OIG identified that DMDC personnel did not implement sufficient security design and configuration controls over DEERS and its operating system to limit risks to the DEERS security posture. DMDC personnel could not substantiate whether [redacted] because the development steering group did not document its informal evaluations.

We evaluated whether controls were designed and effectively implemented over DEERS to deter and protect sensitive data from compromise by internal and external cyber threats. We determined DMDC management did not implement 33 information assurance controls for protecting DEERS from internal and external cyber threats. Specifically, 16 information assurance controls were applicable to protecting DEERS security posture, 11 information assurance controls related to unauthorized access to DEERS, and 6 information controls related to DEERS configuration management. The 33 information assurance controls resulted in 32 recommendations. The DoD OIG determined that all 32 recommendations were acted upon and closed between 2012 and 2017. See appendix B for listing of recommendations and DMDC responses.

Review of Internal Controls

~~(FOUO)~~ DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[4] We identified internal control weaknesses related to DEERS cybersecurity controls. Specifically, DMDC personnel did not implement [redacted], establish an out-processing process and appoint trusted agents, implement a standard schedule for scans, and verify and document the operational functionality of all [redacted]. We will provide a copy of the report to the senior official responsible for internal controls in the Office of the Under Secretary of Defense for Personnel and Readiness.

[4] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

DMDC Improved DEERS Cybersecurity Controls But Additional Action Was Needed

The Director, DMDC, took corrective actions to close 28 of the 32 recommendations issued. Specifically, DMDC management updated cybersecurity policies and procedures, implemented physical security controls for the data center, and obtained data sharing agreements.

~~(FOUO)~~ However, we identified that the Director, DMDC, did not take agreed-upon actions for Recommendations A.3, B.1.e, B.1.f, and C.6. Specifically, the Director did not implement [redacted], establish a centralized procedure for out-processing personnel, identify and appoint trusted agents for completing out-processing procedures for terminated personnel in a timely manner, or validate the [redacted].[5] This occurred because:

- ~~(FOUO)~~ DMDC personnel [redacted] in place of using the automatic update feature because the DEERS servers have limited connectivity to the DoD Non-secure Internet Protocol Router Network,
- the DMDC Division Director relied on Employee Action Request Forms (EAFs) to out-process personnel and did not establish a centralized out-processing method,
- the DMDC Division Director EAF process did not include trusted agents for completing out-processing actions, and
- ~~(FOUO)~~ the DMDC Information System Security Officer did not implement a standard schedule for scans to verify and document the operational functionality of all [redacted].

~~(FOUO)~~ During the audit, the Director, DMDC, agreed to acquire software to enable [redacted], establish a centralized process for out-processing terminated personnel, identify and appoint trusted agents accountable for timely removing employee network access, and identify [redacted]. The Director's agreed upon actions if implemented should address recommendations A.3, B.1.e, B.1.f, and C.6 from the original report. Therefore, this report contains no additional recommendations.

[5] Ports provide electronic connection points and protocols establish the rules to move data from point to point.

DMDC officials need to implement cybersecurity measures immediately to fully protect personally identifiable information from constantly evolving threats and security weaknesses. Until DMDC increases their security posture DEERS will continue to be vulnerable to increased cyber attacks that could jeopardize the integrity and confidentiality of sensitive DEERS data.

DMDC Management Action Taken

We determined that DMDC management took actions to address 28 of 32 recommendations made in Report No. DODIG-2012-090. Of the 28 recommendations addressed, 6 related to configuration management, 6 related to access controls, 4 related to program management, 3 related to physical environment protection, 3 related to audit accountability, 4 related to security assessment and authorization, and 2 related to system communication. During our review, we:

- ~~(FOUO)~~ verified that DMDC officials implemented the [redacted] automated monitoring tool and observed that the tool produced audit logs documenting that system security requirements were being followed by DMDC personnel;
- verified that the Information System Security Officer reviewed and documented all system application changes before deployment;
- conducted physical inventory checks to verify that the DMDC Configuration Management Database server and related equipment entries were accurate and complete; and
- Verified documentation from the role-based control tracking system to validate that personnel with privileged access to DMDC data and network centers completed the requirements to maintain continued access.

We provide detailed examples of verified management actions taken below.

Cybersecurity Policy Updated

In July 2017, the DMDC Information System Security Manager updated the DMDC Cybersecurity Policy to require officials to:[6]

- perform vulnerability assessments;
- document and submit vulnerability assessment results to the Information System Security Officer;

[6] DMDC Cybersecurity Policy, July 27, 2017

- prepare and approve formal risk assessments before outsourcing key cybersecurity services;
- document evaluations that support the risk of using public domain software;
- implement policies and procedures for managing, configuring, and securing the DMDC network devices; and
- establish procedures for granting access, including remote access, to DMDC systems and resources.

We reviewed the DMDC Cybersecurity Policy, conducted personnel interviews, and performed observations of physical and environmental protections, access controls, and system scanning. We performed testing on the verification of public domain software and remote access agreements and based on our review determined the policy updates addressed all specifics for recommendations A.1.a, A.1.b, A.1.c, A.1.d, A.8, and B.1.j.

Data Center Physical Security Controls Enhanced

~~(FOUO)~~ In May 2012, the DMDC enhanced the physical security controls at its data center. Specifically, the DMDC [redacted]. NIST SP 800-53 states that the organization enforces physical access authorizations by controlling ingress and egress to the facility.[7] The previous DoD OIG report stated that the DMDC data center lacked physical security measures to protect the data center. We observed that the DMDC [redacted]. In addition, we reviewed [redacted]. DMDC Director addressed all specifics of the recommendation; therefore, recommendation B.1.l is closed.

Data Sharing Agreements Established

We reviewed 215 DMDC data sharing agreements and determined that the agreements were current and signed by both organizations. NIST SP 800-47 states that agreements, such as memorandums of agreement, governing the interconnection of systems prescribe the terms and conditions for sharing data and information resources in a secure manner.[8] We reviewed the listing of

[7] DoD Instruction 8510.01, "Risk Management Framework," March 12, 2014, states that all DoD information systems must be categorized in accordance with Committee on National Security Systems Instruction 1253 and implement a corresponding set of security controls from NIST SP 800-53.

[8] NIST SP 800-47, "Security Guide for Interconnecting Information Technology System," August 2002.

organizations with a need for access to DEERS and compared the listing to the master file to determine whether all of the agreements were on file and updated within the last 6 years. We determined that all 215 data sharing agreements on file were current and signed by both the agency and the Director, DMDC, as required by the NIST. DMDC Director addressed all specifics of the recommendation; therefore, recommendation B.1.k is closed.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ DMDC management [redacted].

~~(FOUO)~~ Personnel from the Office of the DMDC Chief Information Officer [redacted].

~~(FOUO)~~ On July 10, 2017, we requested the manual [redacted].

~~(FOUO)~~ NIST SP 800-83 states that malware (such as viruses, worms, and Trojan horses) has become the greatest external threat to most information systems.[9] [redacted]

[9] NIST SP 800-83, Revision 1 “Guide to Malware Incident Prevention and Handling for Desktops and Laptops,” July 2013.

~~(FOUO)~~ [redacted].

Out-Processing Procedures Were Not Centralized

~~(FOUO)~~ DMDC management did not establish a centralized process for out-processing and reporting, implement role-based access controls, or perform periodic cybersecurity audits in accordance with the DMDC Cybersecurity Policy. This occurred because the DMDC Division Director relied on Employee Action Request Forms (EAFs) to out-process personnel and did not establish a centralized out-processing procedure. The DMDC account managers took an average [redacted]. If terminated personnel continue to have access to the DEERS network, the network will remain vulnerable to attacks and manipulation.

DMDC management did not establish a centralized process for out-processing and reporting. DMDC management did not implement a timely centralized for out-processing and reporting that enables DMDC management to have reliable information to make informed decisions for out-processing terminated personnel. In addition, DMDC personnel did not perform audits or implement a role-based access control feature restricting system access to unauthorized users based on the termination date. The role-based access control is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. The DMDC Cybersecurity Policy mandates that personnel from the Office of the Chief Information Officer disable inactive accounts after 30 days and delete them after 45 days. The policy mandates that the Information System Security Officer audit user accounts and associated access controls to ensure validity and accuracy, and identify dormant accounts. The Information System Security Officer could not support that a role-based access control was in place to ensure that personnel from the Office of the Chief Information Officer disabled inactive personnel accounts after 30 days and deleted them after 45 days. In addition, the Information System Security Officer could not support that audits were completed.

~~(FOUO)~~ This occurred because the DMDC division director relied on EAFs to out-process personnel and did not establish a centralized out-processing procedure. The DMDC account managers took an average [redacted]. DMDC management relied on employee supervisors to send EAFs to 15 account managers in systems, technical, and operations support divisions. The EAFs provides account managers with the account access actions

~~(FOUO)~~ to be taken, such as in-processing and out-processing and change and move notifications. We requested a list of terminated personnel from January 2017 to June 2017, and DMDC personnel provided a list of 94 terminated personnel. DMDC personnel could provide [redacted]. We notified DMDC officials on June 19, 2017, and the DMDC Information Technology specialist [redacted]. However, on June 20, 2017, [redacted]. In February 2018, the Information Technology Operations Division personnel updated the status for [redacted] completed appropriate actions.

~~(FOUO)~~ DMDC account managers [redacted]. The Director, DMDC, should implement a centralized process to out-process personnel effectively and in a timely manner.

Trusted Agents Were Not Appointed

In February 2018, DMDC management did not provide documentation to the audit team that supports whether personnel performed quarterly audits to verify access revocation or whether trusted agents were appointed for completing out-processing for terminated personnel in a timely manner. DMDC management relied on the employee supervisors to submit EAFs for network access removal and account deactivation. The DEERS network will remain vulnerable to attack and manipulation if terminated personnel continue to have access to the network.

~~(FOUO)~~ The DMDC Cybersecurity Policy states that the Systems Division will revoke [redacted] accounts immediately upon personnel departure; personnel from the Office of the Chief Information Officer will delete such accounts no later than 30 days after the termination date set forth in the EAFs. If an employee terminates under adverse circumstances, the DMDC Information Systems Security Division will revoke all system access at time of employee notification of termination. However, the DMDC Information System Security Officer was unable to provide EAFs and other documentation to support whether personnel conducted quarterly audits of randomly selected

~~(FOUO)~~ separated individuals to verify access had been revoked. In addition, the DMDC Chief Information Officer did not identify or appoint trusted agents responsible for out-processing personnel in a timely manner. This occurred because DMDC management relied on supervisor EAF submissions for network access removal and account deactivation to the Information System Security Officer. The DMDC Information System Security Officer could not provide documentation to support whether terminated personnel deactivations were occurring in a timely manner in accordance with the DMDC Cybersecurity Policy. From January 2017 to June 2017, DMDC personnel took an average [redacted].

During the 2012 audit, DMDC employed trusted agents but the responsibility for processing the terminated personnel was not assigned and not included in DMDC policies until 2017 when DMDC issued its Cybersecurity Policy that requires contractor trusted agents to out-process contractor personnel only. DMDC management did not demonstrate the involvement of trusted agents in ensuring the out-processing procedures for terminated employees were completed. If terminated personnel continue to have the ability to achieve unauthorized access to the DEERS network, DEERS data remains vulnerable to manipulation. The Director, DMDC, should appoint trusted agents to out-process DMDC personnel and hold individuals accountable for removing employee network access in accordance with the DMDC Cybersecurity Policy requirements.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ The DMDC Information Technology Operations personnel [redacted].

~~(FOUO)~~ During our site visit, DMDC personnel [redacted]. The Defense Information Systems Agency (DISA) requires all ports used internally or externally, to be registered and listed on its Category Assurance List.[10]

[10] The Category Assurance List is a collective list of standard ports, protocols, services, network boundary combinations approved for use within the DoD on classified and unclassified networks.

DISA require DoD organizations to provide system information including the name, version number, description, network classification, system type and expiration date when registering their ports.

~~(FOUO)~~ DMDC management should [redacted].[11] DoD Instruction 8551.01, requires ports, protocols, and services not listed in the Category Assurance List be approved by the Ports, Protocols, and Services Management Configuration Control Board.[12] In addition, the instruction requires [redacted].[13] [redacted].

Deficient Cybersecurity Controls Compromise DEERS Information

In February 2017, the Government Accountability Office (GAO) reported that cyber intrusions and attacks on Federal systems and systems supporting our Nation's critical infrastructure, such as communications and financial services, are evolving and becoming more sophisticated. Additionally, consistent shortcomings in the Federal Government's approach to ensuring the security of Federal information systems and cyber critical infrastructure, as well as its approach to protecting the privacy of personally identifiable information, continue to exist.[14] The GAO found that the lack of sufficient security controls compromises the DMDC's capability to protect the sensitive DEERS data for approximately 37 million Service members and DoD civilians from evolving cyber threats.

~~(FOUO)~~ Cyber attacks can originate from within or outside the DMDC. Detection and protection measures must be implemented across the entire DEERS operating environment by implementing the [redacted], establish centralized procedures, identify and appoint trusted agents, and [redacted]. Managing vulnerabilities requires DMDC personnel to regularly evaluate the DEERS operating environment, analyze the results of those evaluations to determine the feasibility of exploiting those

[11] Network traffic that can be analyzed to identify specific internet protocol suite and associated ports.

[12] DoD Instruction 8551.01 "Ports, Protocols, and Services Management," May 28, 2014.

[13] Point at which an enclave's internal network service layer connects to an external network's service layer, i.e., to another enclave or to a Wide Area Network.

[14] See Appendix A for more details.

vulnerabilities, and mitigate potential weaknesses by implementing required security patches or introducing additional controls. If DMDC personnel do not continuously monitor the effectiveness of controls designed and implemented to strengthen the DEERS security posture, hackers can exploit vulnerabilities that jeopardize the integrity and confidentiality of sensitive DEERS data. Even though DMDC management implemented 28 recommendations, management did not fully implement corrective actions to address the remaining 4 recommendations. DMDC personnel should take prompt actions to minimize malware and insider threats, which can result in the loss or manipulation of sensitive data.

Recommendations, Management Actions Taken, and Our Response

Recommendation 1

We recommend that the Director, Defense Manpower Data Center:

a. **~~(FOUO)~~ Update the Defense Enrollment Eligibility Reporting System server [redacted] in accordance with NIST SP 800-53 requirements.**

Management Actions Taken

~~(FOUO)~~ On July 20, 2017, we met with the Director, DMDC, to discuss our preliminary findings. We notified the Director that [redacted].

~~(FOUO)~~ On September 21, 2017, DMDC management stated that personnel from the Office of the Chief Information Officer had implemented [redacted]. Additionally, DMDC management [redacted]. DMDC management stated that the [redacted]. The Director stated that personnel from the Office of the Chief Information Officer would [redacted]. DMDC management plans to complete corrective actions or provide a status update on their progress by April 16, 2018.

Our Response

~~(FOUO)~~ The actions the Director, has initiated should address the specifics of the recommendation therefore, the 2012 report recommendation A.3 is resolved. We will close the recommendation once we verify that DMDC personnel have implemented [redacted].

b. **Establish a centralized procedure for out-processing terminated personnel.**

Management Actions Taken

On July 20, 2017, we notified the Director, DMDC, that the DMDC did not have a centralized procedure for out-processing personnel. The Director acknowledged the DMDC's lack of a centralized procedure for out-processing personnel and agreed to re-evaluate and develop procedures in 45 days for the centralized process.

On December 12, 2017, the DMDC started working with the Headquarters Defense Human Resources Activity Human Resources Directorate to establish a centralized procedure for out-processing terminated, separated, or retired personnel.

Our Response

The actions initiated by the Director, once completed, should address all specifics of the recommendation; therefore, the recommendation from the 2012 report is resolved and remains open. We will work with DMDC management to obtain completion dates for planned actions. We will close the recommendation once we verify that DMDC personnel have implemented a centralized process for out-processing personnel.

c. **Identify and appoint trusted agents responsible for revoking access for out-processing terminated personnel.**

Management Actions Taken

On July 20, 2017, we notified the Director, DMDC, that we could not identify whether DMDC management had appointed trusted agents responsible for revoking access for out-processing terminated personnel. The Director acknowledged the DMDC's lack of trusted agents and agreed to reevaluate the current procedures, including identifying trusted agents, and to review current personnel rules to hold trusted agents accountable for completing employee out-processing actions. DMDC management plans to complete corrective actions by April 16, 2018, or provide a status if not completed by April 16, 2018.

Our Response

~~(FOUO)~~ The actions the Director plans to initiate should address the specifics of the recommendation; therefore, the 2012 report recommendation B.1.f is resolved. We will close the recommendation once we verify that DMDC personnel have implemented standard operating procedures holding trusted agents accountable for timely removal of employee network access.

d. ~~(FOUO)~~ [redacted]

Management Actions Taken

~~(FOUO)~~ On July 20, 2017, we met with the Director, DMDC, to discuss our preliminary findings. We notified the Director, DMDC, of the DEERS servers' [redacted]. The Director agreed to justify [redacted] [redacted]. DMDC management plans to complete corrective actions by April 16, 2018, or provide a status if not completed by April 16, 2018.

Our Response

~~(FOUO)~~ The actions the Director plan to initiate should address all specifics of the recommendation; therefore, the 2012 report recommendation C.6 is resolved. We will close the recommendation once we verify that DMDC personnel have justified or [redacted].

Appendix A

Scope and Methodology

We conducted this performance audit from April 2017 through March 2018 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We visited the DMDC in Seaside, California, and Alexandria, Virginia, and the DISA Defense Enterprise Computing Center in Columbus, Ohio. We assessed the DMDC's efforts to implement the recommendations in Report No. DODIG-2012-090 and determined whether corrective actions addressed the recommendation. The report identified 33 physical and cybersecurity internal control weaknesses for protecting DEERS from internal and external cyber threats that resulted in 32 recommendations. Specifically:

- 16 security posture internal control deficiencies resulted in 13 recommendations;
- 11 unauthorized access internal control deficiencies resulted in 13 recommendations; and
- 6 configuration management internal control deficiencies resulted in 6 recommendations.

Interviews and Documentation

We interviewed personnel from the Information Technology Operations and Cybersecurity Branch responsible for managing and implementing information security over the DMDC network and DEERS, including the Information System Security Manager, Information System Security Officer, and Information Security Specialists.

We conducted walkthroughs of DMDC Seaside and DISA Defense Enterprise Computing Center facilities to evaluate physical and environmental controls for data centers hosting the DEERS servers. We interviewed the DMDC Seaside data center manager, as well as the DISA Defense Enterprise Computing Center site security managers and network engineer (contractor) to determine how both organizations managed access to the data centers and protected the DEERS operating system from environmental damage.

In addition, we interviewed the DEERS Director, Cybersecurity, and the DMDC Seaside Data Center Manager to discuss the DEERS configuration management processes.

We obtained and analyzed the following Federal and DoD Policy and guidance to determine whether the DMDC followed the policies to remediate physical and cybersecurity weaknesses identified in Report No. DODIG-2012-090:

- NIST Special Publication 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” April 2013, Incorporating Updates as of January 22, 2015;
- NIST Special Publication 800-30, “ Guide for Conducting Risk Assessment,” September 2012;
- DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology,” May 24, 2016.

We reviewed the following DMDC standard operating policies and guidance to determine whether applicable guidance was updated and followed.

- Information Assurance Policy, February 19, 2014;
- Cybersecurity Policy, Revision 3, June 20, 2017;
- Audit and Accountability Program, Plan, and Procedures, May 31, 2017;
- Organizational Configuration Management Plan, June 1, 2017;
- Vulnerability Assessment Policy, August 23, 2016;
- Assured Compliance Assessment Solution Scanning Standard Operating Procedure, August 19, 2016;
- Information Technology Service Management Change Management Technical Review Board and Change Control Board Process, July 18, 2017.

We reviewed the DEERS and DMDC documentation to determine whether all data were complete and accurate:

- Contracts, DMDC and DISA service-level agreements;
- Appointment letters, Plan of Action and Milestones, vulnerability scans;
- Open port scans, interconnection memorandums of understanding;
- Network diagrams, audit logs, System Authorization Access Request (DD Form-2875), EAFs; and
- Solaris UVSCAN Virus signature server feasibility to determine the effectiveness of the DMDC’s implementation of DEERS cybersecurity controls.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Use of Technical Assistance

DoD OIG Quantitative Methods and Analysis Division provided assistance in developing our methodology for selecting nonstatistical samples.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the DoD OIG issued three reports discussing DEERS and cybersecurity infrastructure. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

GAO

Report No. GAO-17-440T, "Cybersecurity Actions Needed to Strengthen U.S. Capabilities," February 14, 2017

> The GAO has consistently identified shortcomings in the Federal Government's approach to ensuring the security of Federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information. While previous administrations and agencies have acted to improve the protections over Federal and critical infrastructure information and information systems, the Federal Government needs to take the following actions to strengthen U.S. cybersecurity:
>
> - Effectively implement risk-based entity-wide information security programs consistently over time;
> - Improve its cyber incident detection, response, and mitigation capabilities;
> - Expand its cyber workforce planning and training efforts;
> - Expand efforts to strengthen cybersecurity of the Nation's critical infrastructures; and
> - Better oversee protection of personally identifiable information.

DoD OIG

Report No. DODIG-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012[15]

Report No. DODIG-2012-069, "Action is Needed to Improve the Completeness and Accuracy of DEERS Beneficiary Data" April 2, 2012

> The DEERS beneficiary supporting documentation was not complete, and DEERS data were not always accurate. Specifically, of the 9.4 million Uniformed Service beneficiary records, DEERS supporting documentation did not adequately:
>
> - substantiate the identity of 2.1 million beneficiaries;
> - demonstrate the eligibility of 2.8 million beneficiaries;
> - support one or more critical data fields for 5.7 million beneficiaries; and
> - contain date of birth, gender, name, or relationship records of 199,680 beneficiaries.

[15] See Appendix B for recommendations and agreed-upon actions.

Appendix B

Report No. DODIG-2012-090 Recommendations and Agreed-Upon Actions

In Report No. DODIG-2012-090, the DoD OIG recommended that the Director, DMDC, take action to implement additional cybersecurity controls over DEERS. The recommendations and the Director's agreed-upon actions for each recommendation are as follows:

~~(FOUO)~~ **Recommendation A.1.a:** Update the DMDC Information Assurance Policy, November 4, 2009, to require Systems and Technical Support Division personnel to perform regular, at least monthly, vulnerability assessments on all operating systems to verify whether required security patches, critical updates, and Information Assurance vulnerability alert solutions have been applied and addressed in a timely manner. The Director, DMDC, provided an updated Information Assurance Policy and standard operating procedure that included a requirement to scan the DMDC systems on a daily and weekly basis. Additionally, the Director stated that [redacted] was in place as of mid-June 2012. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2013.

Recommendation A.1.b: Update the DMDC Information Assurance Policy, November 4, 2009, to require Systems and Technical Support Division personnel formally document and submit the results of periodic vulnerability assessments to the DMDC Information Systems Security Group to ensure it properly manages known vulnerabilities affecting the agency's information systems. The Director, DMDC, provided an updated Information Assurance Policy and standard operating procedure that included a requirement to scan the DMDC systems on a daily and weekly basis. Additionally, the Director, DMDC conducts weekly vulnerability assessments, provides the results to the DMDC System Division for disposition, and monitors all remedial activities. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2013.

Recommendation A.1.c: Update the DMDC Information Assurance Policy, November 4, 2009, to require System owners to prepare formal risk assessments that are approved by the DMDC Chief Information Officer before outsourcing key Information Assurance services. The Director, DMDC, provided an updated Information Assurance Policy detailing procedures to complete a risk assessments. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2013.

Recommendation A.1.d: Update the DMDC Information Assurance Policy, November 4, 2009, to require Technology Steering Group personnel formally document evaluations that support the risk of using public domain software on DMDC information systems and that are approved by the DMDC Accrediting Authority. The Director, DMDC, provided an updated Information Assurance Policy which included a DMDC Security Checklists for assertions of whether public domain software is included and statements requiring formal "Acceptance of Risk" by the DMDC Designated Approval. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2013.

~~(FOUO)~~ **Recommendation A.2:** Perform penetration testing of the DEERS to verify DMDC management actions are sufficient for mitigating the risk of cyberattacks against the system. The Director, DMDC, initiated [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in October 2015.

~~(FOUO)~~ **Recommendation A.3:** Complete ongoing evaluations to [redacted]. In March 2012, the Deputy Director stated that the DMDC implemented [redacted]. The Deputy Director also stated that the DMDC implemented [redacted]. Additionally, Deputy Director stated that the DMDC's Cyber Command unit was implementing [redacted]. The Deputy Director estimated that this capability would be in place no later than January 2014. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in May 2014. However, during our current audit we determined that additional actions were needed to address this recommendation. See report Finding on page 4.

~~(FOUO)~~ **Recommendation A.4:** Encrypt sensitive DEERS data at rest in accordance with the DMDC Information Assurance Policy, November 4, 2009. The Director, DMDC, stated the Information System Security Officer initiates a series of benchmark tests comparing times to access [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in April 2017.

~~(FOUO)~~ **Recommendation A.5:** Perform a review to determine the staffing requirements and acquire automated tools needed to support the DMDC ability to monitor audit logs supporting DEERS operations. The Director, DMDC, acquired [redacted] in February 2017, as an automated tool to monitor audit logs. Additionally, DMDC provided support for how DMDC determined the correct staffing requirements. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in June 2017.

~~(FOUO)~~ **Recommendation A.6:** Implement additional safeguards and procedures to protect the integrity of DEERS [redacted] audit logs from system administrator actions that could bypass or negate existing security controls over the system. The Director, DMDC, implemented standard operating procedures in November 2012, requiring two System Administrators be present when audit logs are accessed with root privilege, and requiring the observing System Administrator to make a manual log entry that lists actions performed by the primary System Administrator. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in April 2017.

~~(FOUO)~~ **Recommendation A.7:** Configure all DEERS servers with fully functional auditing capabilities that allow all auditable data necessary to reconstruct the events of a security incident to be recorded. The Director, DMDC, [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation A.8: Develop policy and procedures for managing, configuring, and securing DMDC network devices. The Director, DMDC, provided separate standard operating procedures for managing, configuring, and securing DMDC network devices. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in May 2014.

~~(FOUO)~~ **Recommendation A.9:** Deploy host-based intrusion detection systems on the [redacted], contingency failover, and test servers not currently protected by these security devices. The Director, DMDC, installed host-based intrusion detection systems on the [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation A.10: Review the performance of the officials responsible for managing the DMDC Information Assurance program, including the DEERS security posture, and based on the results consider corrective actions, as appropriate to meet DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003, Information Assurance requirements. The Director, DMDC, appointed a new Chief Information Officer, new Chief Enterprise Architect, and new Information System Security Manager and revised DMDC cybersecurity architecture to provide greater oversight of security operations. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2013.

Recommendation B.1.a: Develop a process to accurately account for, and periodically review, at least annually, the DMDC and Service Management Center Auburn Hills personnel with logical access to the DEERS' operating system. The Director, DMDC, implemented a semiannual review in June 2012 to re-verify personnel with DEERS access for privilege level, formal need to know justification, and vetting levels; and used a role-based Access Tool to track compliance reviews semiannually during October and April. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2012.

Recommendation B.1.b: Update the "Guide to Application Security Management," January 18, 2008, for granting access to DEERS applications to specify documentation requirements for a site to obtain access to those applications, to include application managers and site security manager's responsibilities for maintaining and periodically reviewing the documentation to support whether site access had been properly authorized. The Director, DMDC, updated "The Guide to Application Security Management," June 2012, to address the responsibilities of Application Managers with respect to vetting and verification of Site Security Managers. The DoD OIG considered the DMDC actions responsive to the recommendation and closed the recommendation in September 2012.

~~(FOUO)~~ **Recommendation B.1.c:** Review configuration settings to validate whether the [redacted]. The Director, DMDC, stated that [redacted]. Additionally, the DMDC Information Assurance Policy was updated to require [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2013.

Recommendation B.1.d: Appoint, in writing, system administrators, database administrators, and other DMDC personnel performing Information Assurance roles and responsibilities in accordance with requirements in DoD Instruction

8500.2, “Information Assurance Implementation,” February 6, 2003, and DoD Manual 8570.01, “Information Assurance Workforce Improvement Program,” April 20, 2010. The Director, DMDC, appointed, in writing, the Information Assurance Manager and all Information Assurance Officers and included their roles and responsibilities. Additionally, system administrators, database administrators, and other DMDC personnel Information Assurance roles or responsibilities are addressed by submission, receipt, and retention of DD-2875 forms. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2013.

Recommendation B.1.e: Comply with existing out-processing procedures and documentation requirements defined in the DMDC Information Assurance Policy, November 4, 2009, and establish a centralized process to validate whether required actions have been properly taken. In September 2012, DMDC management stating that the DEERS Information Assurance Officer keeps the DEERS DMDC roster current with all EAFs and revokes certificates no later than close-of-business effective separation date. DMDC management stated that all privileged access has been set up for periodic audit in the role-based access control application. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2012. However, during our current audit we determined that additional actions were needed to address this recommendation. See report Finding on page 4.

Recommendation B.1.f: Define a reasonable period of time to promptly deactivate and remove network access and hold trusted agents accountable for completing those actions within that period. In September 2012, DMDC management stated that the scope of the trusted agent is limited and certificate revocations are never processed through the DMDC Unicenter. DMDC management stated that ensuring proper out-processing actions will require verified, formal audit of every out-processing revocation of access permissions, certificates and return of physical assets for all terminated DMDC civilian and contractor personnel. DMDC management offered an alternative action to conduct a quarterly audit of a randomly selected set of 25 terminations. DMDC management stated that the implementation of the formal audits was completed on June 28, 2012. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2012. However, during our current audit we determined that additional actions were needed to address this recommendation. See report Finding on page 4.

Recommendation B.1.g: Review existing contractor e-mail accounts to verify whether they have been properly configured to include a ".ctr" affiliation display. The Director, DMDC, corrected the eight e-mail accounts without an appropriate affiliation display, fulfilling compliance in October 2012, with the shift of responsibility from the DMDC to the DISA Identify Synchronization Service for creating e-mail addresses. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

~~(FOUO)~~ **Recommendation B.1.h:** Reconcile and periodically, at least annually, revalidate whether personnel with access to the DMDC Seaside data center continue to need access to that facility, and require them to complete a DMDC user agreement. The Director, DMDC, implemented a documented process for [redacted] personnel with such access. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

~~(FOUO)~~ **Recommendation B.1.i:** Review and periodically, at least annually, revalidate existing accounts for the DMDC and Service Management Center Auburn Hills personnel with physical and logical access to DEERS servers and databases, and reconcile those accounts to verify whether access was granted based on approved user access request forms. The Director, DMDC, [redacted] by the Information Systems Security Officer. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

~~(FOUO)~~ **Recommendation B.1.j:** Revise and update existing procedures for granting access to DMDC systems and resources, to include remote access that address requirements for:

- periodically revalidating the continued need for access;
- supervisory review and documented approval of access; and
- justifying the need and level of access requested.

The Director, DMDC, [redacted] by the Information Assurance Officer. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation B.1.k: Develop new or update existing data sharing agreements to verify whether agreements are in place that describe security requirements and the terms and conditions for transferring data between organizations authorized to receive DEERS data. The Director, DMDC, rewrote all memorandum of understandings/data use agreements to be more specific on breach reporting, encryption and data auditing. The audit team verified 224 agreements were current and signed. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in June 2017.

~~(FOUO)~~ **Recommendation B.1.l:** Implement appropriate security measures to fully protect unsecured access points to the DoD Center Monterey Bay data center. The Director, DMDC, [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation B.2: We recommend that the Director, DMDC, in coordination with the contracting officer, review the performance of the contracting officer's representative responsible for providing oversight of contract HC1028-08-D-2018, September 4, 2008, and based on the results, consider any corrective action, as appropriate. The Director, DMDC, provided documentation showing proper oversight and monitoring of contracts by the contracting officer's representative. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2012.

Recommendation C.1: Revise the DMDC Organizational Configuration Management Plan, Version 4.2, January 2009, the DEERS Configuration Management Plan, Version 4.2, January 2009, and the Information Technology Service Management Change Management Technical Review Board and Configuration Control Board Process, November 9, 2010, to require documented results supporting whether proposed configuration changes affect the security posture of all the DMDC information systems, including DEERS. The Director, DMDC, altered the DMDC Configuration Management Plan and Technical Review Board and Configuration Control Board process documentation, and the documentation now encompasses all application changes for all the DMDC Divisions. The Information System Security Officer is designated to review all application changes pre-deployment. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation C.2: Revise the Information Technology Service Management Change Management Technical Review Board and Configuration Control Board Process, November 9, 2010, to require all proposed system hardware changes to be properly tested and the results of testing documented before the system hardware

Configuration Control Board approves the changes to be implemented in the production environment. The Director, DMDC stated that the DEERS Information System Security Officer reviewed all proposed change specifications and verified Systems personnel post a full hardware-test standard operating procedure. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation C.3: Include the DMDC Information System Security Manager or his written designee as an active and required member of the application and system hardware Configuration Control Boards. The Director, DMDC, stated that the Information System Security Manager or an approved delegate is designated in the Technical Review Board and Configuration Control Board Charter as an official member of both system hardware and software Configuration Control Boards. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

Recommendation C.4: Update the existing DMDC enterprise-wide system hardware and software inventories to include sufficient information that enables Systems and Technical Support Division personnel to maintain a comprehensive configuration baseline of DEERS-specific system hardware and software. The Director, DMDC, updated the DMDC's existing system databases, including accreditation boundaries using system hardware and software, with the Information Systems Security Officer verifying the Configuration Management Database and has accounted properly for all DEERS servers in the accreditation boundary. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in September 2012.

~~(FOUO)~~ **Recommendation C.5:** Develop and implement procedures to account for system hardware throughout the complete life cycle of the equipment, including hard drives, that process or store sensitive DEERS data. The Director, DMDC, stated that the DEERS Information Systems Security Officer developed an inventory form, spreadsheet, and standard operating procedures, with memory-tracking procedure being published as [redacted]." The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in February 2013.

~~(FOUO)~~ **Recommendation C.6:** Verify and document the operational functionality of all [redacted]. In May 20, 2014, the Deputy Director stated that [redacted] [redacted] cleanup was achieved on or before March 1, 2014. Furthermore, [redacted]. The DoD OIG considered the DMDC action responsive to the recommendation and closed the recommendation in May 2014. However, during our current audit we determined that additional actions were needed to address this recommendation. See report Finding on page 4.

Acronyms and Abbreviations

DEERS	Defense Enrollment Eligibility Reporting System
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
EAF	Employee Action Request Form
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
SP	Special Publication

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

~~FOR OFFICIAL USE ONLY~~