

~~FOR OFFICIAL USE ONLY~~

Report No. DODIG-2012-090

May 22, 2012

Inspector General

United States
Department of Defense



Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture

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

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (571) 372-7469.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (571) 372-7469, or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500



DEPARTMENT OF DEFENSE
hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

Acronyms and Abbreviations

CCB	Configuration Control Board
CIO	Chief Information Officer
DEERS	Defense Eligibility Enrollment Reporting System
DISSG	DMDC Information Systems Security Group
DMDC	Defense Manpower Data Center
IA	Information Assurance
IAO	Information Assurance Officer
IAM	Information Assurance Manager
IDS	Intrusion Detection System
PII	Personally Identifiable Information
SA	System Administrator
SMC	Service Management Center
VPN	Virtual Private Network



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

May 22, 2012

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

SUBJECT: Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture (Report No. DODIG-D2012-090)

We are providing this report for review and comment. Defense Manpower Data Center (DMDC) personnel did not implement adequate information assurance controls to protect the Defense Enrollment Eligibility Reporting System (DEERS) from internal and external physical and cyber threats. ^{DMDC (b)(5)}

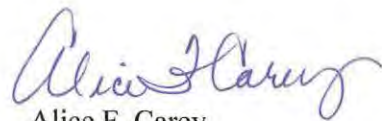
[REDACTED]. We considered DMDC comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. As a result of management comments, we revised draft Recommendation B.1.a, B.1.b, B.1.f, C.1.a, and C.1.b and renumbered draft Recommendation C.1.a, C.1.b, C.2, C.3, C.4, and C.5 as Recommendations C.1, C.2, C.3, C.4, C.5, and C.6, respectively. Comments from the Deputy Director, DMDC, responding on behalf of the Director, DMDC, on Recommendations A.1.a, A.1.b, A.1.c, A.1.d, A.2, A.3, A.5, A.9, A.10, B.1.c, B.1.d, B.1.g, B.1.k, B.1.l, and C.6 were responsive and generally conformed to the requirements of DoD Directive 7650.3, but did not always provide a completion date for the planned actions addressing those recommendations. Therefore, we request the Director, DMDC, provide the completion date of planned actions to Recommendations A.1.a, A.1.b, A.1.c, A.1.d, A.2, A.3, A.5, A.9, A.10, B.1.c, B.1.d, B.1.g, B.1.k, and C.6 by July 20, 2012.

Comments from the Deputy Director, DMDC, responding on behalf of the Director, DMDC on Recommendations A.4, B.1.a, B.1.b, B.1.e, B.1.h, B.1.i, B.1.j, C.3, and C.5 were partially responsive and Recommendations A.6, A.7, A.8, B.1.f, B.2, C.1, C.2, and C.4 were nonresponsive. Therefore, we request the Director, DMDC, provide additional comments on those recommendations by July 20, 2012.

If possible, send a Microsoft Word (.doc) file and a .pdf file containing your comments to audros@dodig.mil. Comments to the final report should be portion-marked in accordance with DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012. Portable document format (.pdf) copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8876 (DSN 664-8876).

A handwritten signature in blue ink that reads "Alice F. Carey". The signature is written in a cursive style with a large initial "A".

Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support



Results in Brief: Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture

What We Did

~~(FOUO)~~ Our objective was to evaluate whether controls were designed and effectively implemented over the Defense Enrollment Eligibility Reporting System (DEERS) to deter and protect sensitive data from compromise by internal and external cyber threats. We reviewed 73 of 107 information assurance (IA) controls that Defense Manpower Data Center (DMDC) implemented.

What We Found

Of the 73 IA controls we reviewed, we did not find weaknesses in how DMDC and Service Management Center Auburn Hills personnel implemented 40 of those controls. However, we found weaknesses in how DMDC personnel implemented ^{DMDC} of the IA controls for protecting DEERS from internal and external cyber threats.

Of the ^{DMDC} deficient controls, ^{DMDC} were applicable to protecting the DEERS security posture. Overall, DMDC personnel did not implement adequate controls for identifying, protecting, and mitigating potential cyber attacks against the DEERS operating system. Specifically, the:

- ~~(FOUO)~~ Systems and Technical Support Division (Systems Division) personnel did not fully protect the DEERS operating system from ^{DMDC} known vulnerabilities because they generally relied on annual IA testing instead of performing regular vulnerability assessments servers, and used ^{DMDC (b)(5)};
- DEERS Division and DMDC Information Systems Security Group (DISSG) personnel did not maintain documentation supporting critical decisions affecting the DEERS security posture because they assessed risk using an unstructured, informal process;
- ~~(FOUO)~~ Systems Division personnel did not create, review, and sufficiently protect audit data affecting ^{DMDC} DEERS servers because DISSG personnel did not assign sufficient

resources for monitoring activity and did not implement additional safeguards to protect the integrity of DEERS audit trails; and

- ~~(FOUO)~~ Systems Division and DISSG personnel did not adequately isolate network security devices and monitor ^{DMDC (b)(5)} DEERS servers for unauthorized activity because they did not develop appropriate policy for managing network devices that addressed installing and monitoring firewalls and intrusion detection systems.

As a result, DMDC's security measures for protecting sensitive DEERS data for approximately 37 million Service members, DoD civilians, retirees, and family members may not fully protect personally identifiable information from evolving threats and security vulnerabilities.

In addition, ^{DMDC (b)(5)} Overall, DMDC personnel did not implement a comprehensive process to verify that only authorized personnel, with a valid need-to-know, could access DEERS data, its operating system, and the DMDC Seaside data center. Specifically, DMDC personnel did not develop and implement appropriate procedures to account for personnel supporting DEERS operations, including those that perform IA responsibilities, because personnel from the:

- DEERS Division did not maintain current access control lists or verify whether ^{DMDC} application managers responsible for managing access to DEERS applications at ^{DMDC} sites maintained appropriate and accurate documentation and deactivated inactive accounts;
- DISSG misinterpreted DoD policy and did not maintain sufficient documentation to support employee out processing actions for ^{DMDC} personnel;
- DEERS and Systems Divisions did not periodically revalidate access; and

- Systems Division did not appropriately configure ^{DMDC (b)(5)} contractor e-mail accounts.

Also, DMDC personnel did not implement a consistent and structured process for granting and maintaining access to DEERS and DMDC network devices because personnel from the:

- DEERS and Systems Division did not require or maintain written authorization request forms and they did not periodically revalidate access to the ^{DMDC (b)(5)} data center, DEERS operating system, or DMDC network resources;
- ^{DMDC (b)(5)}
- ~~(FOUO)~~ Business Operations and Management Division did not provide effective oversight of contract HC1028-08-D-2018, valued at approximately ^{DMDC (b)(5)}.

~~(FOUO)~~ Additionally, DMDC personnel did not protect all physical points of access to the ^{DMDC (b)(5)} data center because they did not consider the risk of safeguarding ^{DMDC (b)(5)} a priority. As a result, these weaknesses decrease the DMDC's ability to prevent unauthorized access and modification or loss of DEERS data to include personally identifiable information, and other Privacy Act data for 37 million Service members, retirees, family members, and DoD civilians.

Further, ^{DMDC (b)(5)}

Overall, DMDC personnel did not implement sufficient configuration controls to limit risks to the DEERS security posture. Specifically, DMDC personnel:

- could not substantiate whether ^{DMDC (b)(5)} software application and ^{DMDC (b)(5)} system hardware changes affected the DEERS security posture because the Development Steering Group did not document its informal evaluations;
- did not test ^{DMDC (b)(5)} system hardware changes before implementing them in the DEERS production environment because the Technical Review Board subjectively decided whether changes needed to be tested instead of testing all changes;

- had limited accountability of DEERS-specific hardware and software because Systems Division personnel used enterprise-wide processes that did not specify whether the system hardware and software supported DEERS operations; and

~~(FOUO)~~ ^{(b) (7)(E), (b) (5)}

Without stringent configuration management controls, changes could compromise the security and integrity of DEERS by weakening or negating existing security controls, or by introducing new vulnerabilities.

What We Recommend

~~(FOUO)~~ We recommended that the Director, DMDC, appropriately monitor and protect the DEERS operating system by using current virus protection software, deploying host-based intrusion detection systems, logging and reviewing all system activity, and securing unprotected access points to the DMDC Seaside data center; and assess, document, and test whether changes to be implemented in production affect the security posture of DEERS.

Management Comments and Our Response

Based on management comments, we revised five recommendations to clarify the actions required to address weaknesses affecting the DEERS security posture. Comments from DMDC were sometimes responsive. However, DMDC comments were also partially responsive or were nonresponsive to the intent of our recommendations. We request that management provide additional comments and the completion date for the planned actions by ^{DMDC (b)(5)}. Please see the recommendations table on page iii.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Director, Defense Manpower Data Center	A.1.a, A.1.b, A.1.c, A.1.d, A.2, A.3, A.4, A.5, A.6, A.7, A.8, A.9, A.10, B.1.a, B.1.b, B.1.c, B.1.d, B.1.e, B.1.f, B.1.g, B.1.h, B.1.i, B.1.j, B.1.k, B.2, C.1, C.2, C.3, C.4, C.5, C.6	B.1.1

Please provide additional comments and the completion date to planned actions by July 20, 2012.

Table of Contents

Introduction	1
Objective	1
Background on Defense Manpower Data Center and Defense Enrollment Eligibility Reporting System	1
Review of Internal Controls	4
Finding A. Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture	5
(FOUO) DMDC (b)(5)	5
DMDC (b)(5)	
DMDC (b)(5)	9
(FOUO) DMDC (b)(5)	11
DMDC (b)(5)	
DMDC (b)(5)	13
DMDC (b)(5)	
DMDC (b)(5)	
Conclusion	14
Management Comments on the Finding and Our Response	15
Recommendations, Management Comments, and Our Response	17
Finding B. Stronger Controls Needed to Prevent Unauthorized Access	24
DMDC (b)(5)	25
DMDC (b)(5)	29
DMDC (b)(5)	34
Conclusion	35
Management Comments on the Finding and Our Response	35
Recommendations, Management Comments, and Our Response	37
Finding C. Weaknesses Existed in Defense Enrollment Eligibility Reporting System Configuration Management Practices	46
Security Assessments Were Not Documented	46
System Hardware Changes Were Not Always Tested	47
DMDC (b)(5)	48
DMDC (b)(5)	
(FOUO) DMDC (b)(5)	49

Table of Contents (cont'd)

Finding C. Weaknesses Existed in Defense Enrollment Eligibility Reporting System Configuration Management Practices (cont'd)

Conclusion	50
Management Comments on the Finding and Our Response	51
Recommendations, Management Comments, and Our Response	51

Appendices

A. Scope and Methodology	56
Use of Computer-Processed Data	58
Use of Technical Assistance	59
Prior Coverage	59
B. (FOUO) DMDC (b)(5)	60
DMDC (b)(5)	
DMDC (b)(5)	
C. Controls With Weaknesses Affecting the Defense Enrollment Eligibility Reporting System Security Posture	61
D. Controls Without Significant Weaknesses	69

Glossary	79
----------	----

Management Comments

Defense Manpower Data Center	83
------------------------------	----

Introduction

Objective

Our objective was to evaluate whether controls were designed and effectively implemented over the Defense Enrollment Eligibility Reporting System (DEERS) to deter and protect sensitive data from compromise by internal and external cyber threats. See Appendix A for a discussion of the scope and methodology related to the audit objective and Appendix B for a discussion on other matters of interest. See the Glossary for terms used throughout the report.

Background on DMDC and DEERS

The Defense Manpower Data Center (DMDC) is a DoD field activity 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. DMDC maintains the largest archive of personnel and medical benefits, manpower, training, security, and financial data for all Uniformed Service members, retirees, family members, DoD civilians, and select contractors. DMDC is responsible for managing, maintaining, and securing DEERS, which is one of its largest operational programs. In FY 2011, DMDC ^{DMDC (b)(5)} [REDACTED]

[REDACTED] including DEERS operations. DEERS was initially developed in the 1970s as a joint medical and personnel database, but did not become operational until 1982. Since then, DEERS functionality and its mission have evolved as the DoD-designated automated information system supporting the DoD TRICARE Program by collecting and storing data for personnel that are eligible to enroll in benefit and entitlement programs and to prevent and detect fraud and abuse in the distribution of those benefits and entitlements. In addition, DEERS supports the Personnel Identity Protection Program by validating personnel-related information during the common access card issuance process.

DEERS is a centralized DoD data repository containing personnel and medical data, including detailed personnel eligibility information for benefits and entitlements for approximately 37 million Uniformed Service members and retirees and their family members, DoD civilians, and DoD contractors. Additionally, DEERS maintains:

- the right index fingerprint of all eligible personnel in a pay or annuity status who are issued identification cards;
- casualty identification data on members of the Uniformed Services to ensure positive identification of those personnel when deceased and to verify entitlement eligibility of surviving family members; and
- information on Uniformed Services members, discharged members, and retirees to verify their eligibility for Government educational programs.

Operational Roles and Responsibilities for Managing DEERS

~~(FOUO)~~ The DEERS Program Management Office is located at DMDC in Seaside, California (DMDC Seaside). DMDC Seaside manages DEERS functionality, the overall security posture of the system, ~~(b)(5)~~

~~(b)(5)~~ DMDC personnel are responsible for the overall DEERS operating environment, including configuring system hardware and software and maintaining the integrity of DEERS data.

~~(FOUO)~~ Hewlett Packard hosts the DEERS ~~(b)(5)~~ operating system (~~(b)(5)~~) ~~(b)(5)~~ at the Service Management Center (SMC) in Auburn Hills, Michigan (SMC Auburn Hills) under contract HC1028-08-D-2018, September 4, 2008. At SMC Auburn Hills, contractors are responsible for providing physical and environmental protection of the DEERS operating environment and ensuring that system hardware and software changes were properly configured and promptly installed. According to the DEERS Information Assurance Officer (IAO), SMC Auburn Hills personnel provided “hands on” support to DMDC operations and information systems.

Information Assurance Controls

~~(FOUO)~~ DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003, establishes a baseline level of IA controls for all DoD information systems by requiring system owners to assign each system a mission assurance category and confidentiality level. The DMDC Designated Accrediting Authority designated DEERS as a mission assurance category II system that processed sensitive information. As such, the DMDC Information Systems Security Group (DISSG) was responsible for designing and implementing 107 IA controls to provide an integrated, layered protection of DEERS. According to the DMDC IA Policy, IAOs are responsible for monitoring and reporting compliance with those controls for specific systems. DoD Instruction 8500.2 separates the 107 IA controls into 8 distinct subject areas:

- ~~(FOUO)~~ 26 security design and configuration controls;
- ~~(FOUO)~~ 4 identification and authentication controls;
- ~~(FOUO)~~ 34 enclave and computing environment controls;
- ~~(FOUO)~~ 6 enclave boundary defense controls;
- ~~(FOUO)~~ 18 physical and environmental controls;
- ~~(FOUO)~~ 5 personnel controls;
- ~~(FOUO)~~ 12 continuity controls; and
- ~~(FOUO)~~ 2 vulnerability and incident management controls.

~~(FOUO)~~ We reviewed 73 of the 107 IA controls that affected DMDC officials' ability to protect DEERS and to deter potential cyber attacks. See Appendix C for the controls that DMDC personnel did not effectively implement to protect DEERS from internal and external cyber threats. See Appendix D for the controls that DMDC and SMC Auburn Hills personnel implemented without weaknesses. The following table shows the number of controls we reviewed by subject area.

Table. IA Controls Reviewed

DoD Instruction 8500.2 Subject Area	Number of Controls Reviewed
Security Design and Configuration	24
Identification and Authentication	4
Enclave and Computing Environment	29
Enclave Boundary Defense	6
Physical and Environmental	4
Personnel	4
Vulnerability and Incident Management	2
	73

DEERS System Architecture

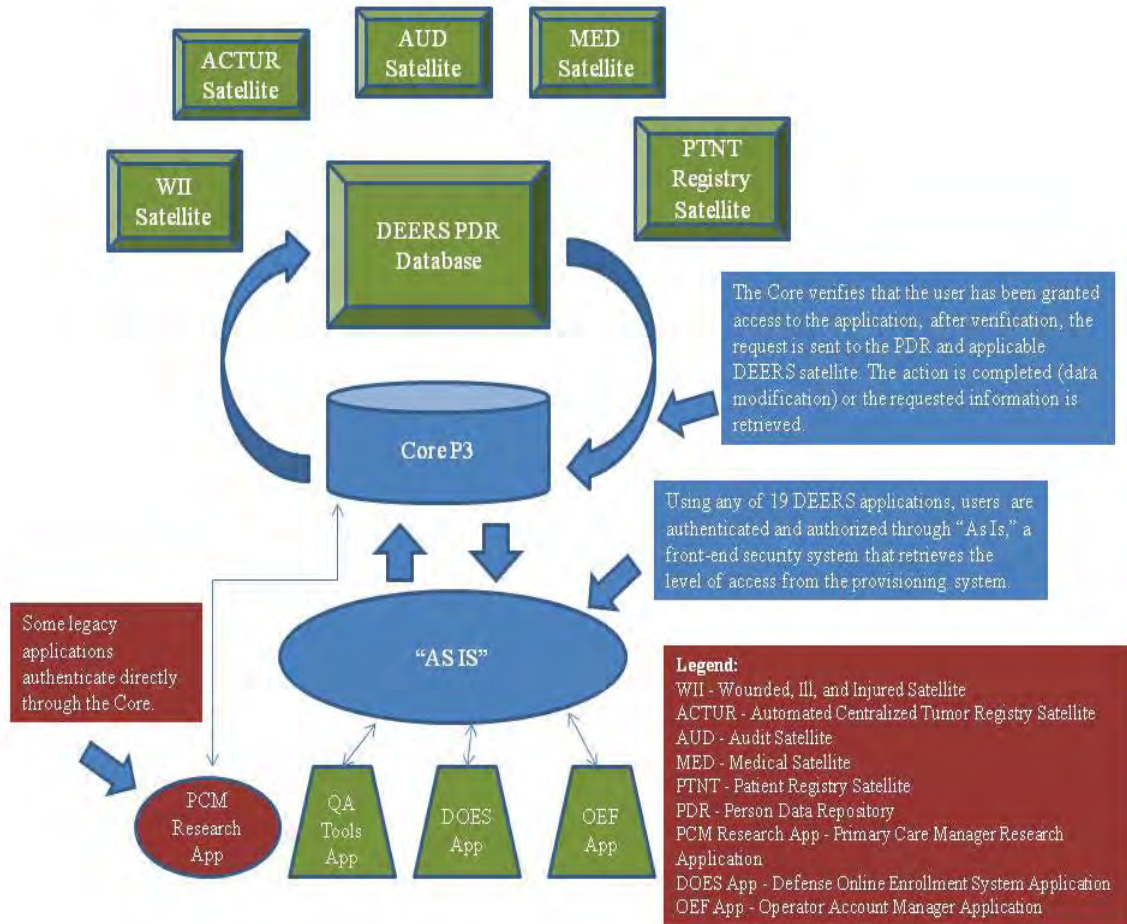
~~(FOUO)~~ The DEERS architecture is comprised of ^{DMDC (b)(5)} [REDACTED] SMC Auburn Hills and DMDC Seaside data centers. Specifically, ^{DMDC (b)(5)} [REDACTED] servers run at the SMC Auburn Hills data center. The remaining ^{DMDC (b)(5)} [REDACTED] DEERS servers that run at the DMDC Seaside data center provide contingency failover operations for the primary production servers at SMC Auburn Hills, testing capabilities, and unique services on one production environment. Currently, DEERS processing takes place through 19 applications that allow personnel in Federal, DoD, and State agencies to view and update existing data or add new data based on predefined levels of access to each application. The DEERS architecture includes the:

- ~~(FOUO)~~ Person Data Repository,¹ which contains personally identifiable information (PII), including names, social security numbers, and dates of birth;
- ~~(FOUO)~~ ^{DMDC (b)(5)} [REDACTED]
- ~~(FOUO)~~ ^{DMDC (b)(5)} [REDACTED].

¹ The DEERS Person Data Repository processes approximately 70 million transactions per month.

Figure 1 represents the process for authentication that DEERS application users follow before accessing DEERS data.

~~(FOUO)~~ Figure 1. DEERS Architecture Description



Source: DoD Office of Inspector General

Review of Internal Controls

~~(FOUO)~~ DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, 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. We determined that internal control weaknesses existed in DMDC. Specifically, DMDC personnel did not perform periodic conformance testing to identify DEERS vulnerabilities; properly configure and secure network-related devices; sufficiently protect all access points to the DMDC Seaside data center; implement a stringent process for granting access to DEERS; and adequately document whether configuration changes affected the overall DEERS security posture. We will provide a copy of the report to the senior official responsible for internal controls in the Office of Under Secretary of Defense for Personnel and Readiness.

Finding A. Improvements Needed to Strengthen the DEERS Security Posture

Of the 73 IA controls we reviewed, we did not find weaknesses in how DMDC and SMC Auburn Hills personnel implemented ^{DM}_{DC} of those controls. However, we found weaknesses in how DMDC personnel implemented ^{DM}_{DC} of the IA controls ^{DMDC (b)(5)}. ^{DMDC (b)(5)}. Of the ^{DM}_{DC} controls we found deficient, ^{DM}_{DC} were applicable to protecting the DEERS security posture.

Although DMDC personnel designed security measures, they did not implement adequate controls for identifying, protecting, and mitigating potential cyber attacks against the DEERS operating system. Specifically, the:

- ~~(FOUO)~~ Systems and Technical Support Division (Systems Division) personnel did not conduct regular tests or fully protect the DEERS operating system from ^{DMDC (b)(5)} known vulnerabilities because they generally relied on annual IA testing instead of performing regular vulnerability assessments on the ^{DM}_{DC} DEERS servers, and used ^{DMDC (b)(5)};
- DEERS Division and DISSG personnel did not maintain documentation supporting critical decisions affecting the DEERS security posture because they assessed risk supporting those decisions using an unstructured, informal process;
- ~~(FOUO)~~ ^{DMDC (b)(5)}
- ~~(FOUO)~~ ^{DMDC (b)(5)}

^{DMDC (b)(5)}

~~(FOUO)~~ ^{DMDC (b)(5)}

~~(FOUO)~~ Although DMDC and SMC Auburn Hills personnel effectively implemented ^{DM}_{DC} of the 73 IA controls we reviewed, weaknesses existed in how DMDC personnel implemented ^{DM}_{DC} of the controls for protecting DEERS from internal and external cyber threats. ^{DMDC (b)(5)}

~~(FOUO)~~ DMDC (b)(5) [Redacted]

~~(FOUO)~~ DMDC (b)(5) [Redacted]

~~(FOUO)~~ DMDC (b)(5) [Redacted]

[Redacted] the information assurance manager (IAM) stated that they were responsible for performing monthly and ad hoc automated scans to identify potential vulnerabilities to the DEERS operating system. DoD Instruction 8500.2 control ECMT-1 (Conformance Monitoring and Testing) requires periodic, unannounced, in-depth monitoring and testing to ensure compliance with all vulnerability mitigation procedures. In addition, the DMDC IA Policy states that DMDC personnel will scan systems on a regular basis to evaluate whether they are susceptible to known vulnerabilities.

~~(FOUO)~~ Although Systems Division personnel were responsible for performing vulnerability scans, the IAM further stated that DMDC generally relied on the results of annual IA testing as its primary basis for identifying known and evolving threats to the overall DEERS security posture. The DMDC IA Policy states that the DISSG, a group within the DMDC Chief Information Office, is responsible for overseeing and implementing information technology security throughout the DMDC enterprise. DMDC (b)(5)

Allowing known vulnerabilities to exist . . . increases the likelihood that sensitive DEERS data could be compromised
DMDC (b)(5) [Redacted]

[Redacted]

Therefore, the DISSG should update the DMDC IA Policy to require personnel to complete and document the results of regular, at least monthly, vulnerability assessments and to provide the results of those assessments to the DISSG to increase its ability to more effectively manage how DMDC personnel mitigate risk.

~~(FOUO)~~ In addition, Systems Division personnel DMDC (b)(5) [Redacted] DoD Instruction 8500.2 control ECMT-1 requires system owners to perform penetration testing to ensure compliance with all vulnerability mitigation procedures. DMDC (b)(5) [Redacted]

(FOUO) DMDC (b)(5) [Redacted]

Although DISSG personnel believed that current processes to identify vulnerabilities provided them with a similar level of assurance, those processes were designed to identify vulnerabilities. DMDC (b)(5)

[Redacted]

(FOUO) DMDC (b)(5) [Redacted]

(FOUO) DMDC (b)(5) [Redacted]

DoD Instruction 8500.2 control VIVM-1 (Vulnerability Management) requires a comprehensive vulnerability management process that includes systematic identification and mitigation of software and hardware vulnerabilities be implemented. DMDC (b)(5)

[Redacted]

(FOUO) In October 2010, an independent contractor completed its annual IA assessment of the DEERS operating environment using Nessus and Retina. DMDC (b)(5)

[Redacted]

² DMDC (b)(5)
³ (FOUO) DMDC (b)(5)
DMDC (b)(5)

(FOUO) DMDC (b)(5) [Redacted]

~~(FOUO)~~ DMDC (b)(5)

~~(FOUO)~~ DMDC (b)(5)



~~(FOUO)~~ DMDC (b)(5)

~~(FOUO)~~ DMDC (b)(5)

~~(FOUO)~~ DMDC (b)(5)

Risk Management Processes and Procedures Needed Improvement

~~(FOUO)~~ Risk management was informal and did not result in DMDC personnel developing documentation necessary to substantiate whether they assessed risk to the overall DEERS security posture. Specifically, DISSG and DEERS Division personnel did not document whether they adequately assessed the risk of using ^{DMDC}_{(b)(5)} contractors to primarily support DEERS operations or using a contractor to perform IAM functions, or ^{DMDC}_{(b)(5)}. In addition, the Technology Steering Group did not document whether they assessed the risk of using ^{DMDC}_{(b)(5)} to support DEERS operations.

Risk Assessments Were Not Performed for Outsourced IA or Key Management Services

~~(FOUO)~~ DISSG personnel did not formally evaluate or document the risk of using contractors to perform key IA services or functions essential to the operational success of the DEERS mission. Specifically, DMDC had seven ongoing contracts in FY 2011, valued at approximately ^{DMDC}_{(b)(5)}, to obtain software development, configuration management, server support, architectural design, and database management, and to host the primary production environment for its systems, including DEERS, at ^{DMDC}_{(b)(5)} ^{DMDC}_{(b)(5)}.

However, documentation assessing the risk of outsourcing those IA services did not exist because DMDC personnel believed their unstructured, informal deliberations were sufficient to show that they had appropriately considered risk when making critical

decisions. DoD Instruction 8500.2 control DCDS-1 (Dedicated IA Services) requires outsourced IA services (such as incident monitoring, analysis and response or key management services) to be supported by a formal risk analysis and approved by the chief information officer (CIO). For example, the DMDC IAM was a contractor from one of the seven contracts DMDC used to support key management services; however, the CIO did not complete or approve a formal, written assessment describing the risks of using a contractor to manage and maintain the DMDC IA program. Although DoD policy does not preclude a contractor from serving in this capacity, DMDC increased its risk associated with using a contractor in this capacity because the IAM was responsible for overseeing the implementation of findings that resulted from same contractor's annual IA assessment.⁶

DMDC increased its risk associated with using a contractor in this capacity because the IAM was responsible for overseeing the implementation of findings that resulted from the same contractor's annual IA assessment.

In addition, the CIO stated that more than ^{DMDC}_{(b)(5)} percent of the personnel supporting DEERS operations were contractors. Documentation provided by DMDC personnel show that

⁶ ~~(FOUO)~~ The IAM was a contractor provided through contract FA8771-04-D-0009, September 15, 2010.

nearly ^{DM DC} percent (^{DMDC (b)(5)}) of the personnel supporting DEERS were contractors. By not formally evaluating the risk of outsourcing such a large percentage of IA support or key management services, the DISSG did not implement a stringent and effective risk management strategy to reduce risk to DEERS operations. Therefore, DISSG personnel should complete formal risk assessments that evaluate the impact proposed actions have on the overall DEERS security posture and obtain CIO approval before entering into future contracts and for continuing to use existing contract services.

(FOUO) ^{DMDC (b)(5)}
(FOUO) ^{DMDC (b)(5)}
[Redacted]

Use of ^{DMDC (b)(5)} Was Not Documented or Approved at the Appropriate Level

(FOUO) DMDC personnel used ^{DMDC (b)(5)} to support DEERS operations. However, the Technology Steering Group did not complete a formal risk assessment or obtain approval from the DEERS Designated Accrediting Authority before using ^{DMDC (b)(5)}. DoD Instruction 8500.2 ^{DMDC (b)(5)} requires management to assess ^{DMDC (b)(5)} for IA impact and obtain approval from the Designated Accrediting Authority before use. DMDC personnel used ^{DMDC (b)(5)}. Although an IAO ^{DMDC (b)(5)} stated the Technology Steering Group assessed the viability of using ^{DMDC (b)(5)}, it did not develop formal documentation because DMDC personnel believed their unstructured, informal deliberations were sufficient to show that they assessed risk.

The DEERS Designated Accrediting Authority was the only official with the authority to formally assume responsibility for ensuring that an information system operated at the proposed level of security. However, an IAO stated that the CIO approved ^{DMDC (b)(5)} for use because the CIO had more technical expertise ^{DMDC (b)(5)}

DMDC (b)(5) DISSG personnel accepted the risk of that type DMDC (b)(5) without approval from the only person authorized to assume such risk to the DEERS security posture. The use of DMDC (b)(5) should only be approved after the DEERS Designated Accrediting Authority is confident that the risks of using DMDC (b)(5) have been thoroughly assessed and documented.

(FOUO) DMDC (b)(5)

(FOUO) DMDC (b)(5)

DMDC (b)(5)

(FOUO) DMDC (b)(5)

(FOUO) DMDC (b)(5)

DMDC (b)(5)

7 (FOUO) DMDC (b)(5)

~~(FOUO)~~ DMDC (b)(5) [Redacted]

~~(FOUO)~~ Because audit trails provide a method to detect intrusions, reconstruct events, establish accountability, and assist in analyzing problems, DMDC (b)(5)

[Redacted]

DMDC (b)(5) [Redacted]

~~(FOUO)~~ The integrity of DEERS DMDC (b)(5) was not sufficiently safeguarded because Systems Division personnel did not implement controls to mitigate the inherent risk associated with DMDC (b)(5). DoD Instruction 8500.2 control DMDC (b)(5)

[Redacted]

8 ~~(FOUO)~~ DMDC (b)(5) [Redacted]

Additional Safeguards Needed to Protect DMDC Network Devices and the DEERS Operating System

~~(FOUO)~~ Systems Division personnel did not sufficiently protect and monitor DMDC network devices and DEERS servers. Specifically, they did not configure DMDC network security devices to logically separate them within the network and monitor

DMDC (b)(5)

Logical Access to DMDC Network Security Devices Was Not Properly Controlled

~~(FOUO)~~ Although the DMDC security support structure, which includes IDSs, firewalls, and other network security devices, was separate from the production environment,

DMDC (b)(5)

DoD Instruction 8500.2 control DCSP-1 (Security Support Structure Partitioning) requires the security support structure to be isolated through the use of partitions or domains and to control access to devices performing security functions. Systems Division personnel did not appropriately configure network security devices to ensure those devices were logically separated from other parts of the network because policy did not exist for configuring network devices within the DMDC enclave as required by DoD Instruction 8500.2 control ECND-2 (Network Device Controls).

DMDC (b)(5)

. Without policy to govern the management of DMDC network devices, inaction by personnel could result in unauthorized personnel accessing or manipulating devices designed to protect the organization from such actions. Therefore, Systems Division personnel should develop policy for properly configuring DMDC network devices and install appropriate firewalls for limiting access to only authorized personnel.

~~(FOUO)~~ VPN Communications Within the DMDC Enclave Were Not Visible to a Network IDS

~~(FOUO)~~ Although external VPN communications were visible to a network IDS, Systems Division personnel did not deploy an IDS to monitor VPN communications within the enclave because DMDC did not develop policy for managing network devices that addressed the use and configuration of those devices. Specifically, the network schematic showed that

DMDC (b)(5)

In addition, DoD Instruction 8500.2 control ECND-2 requires management to implement an effective network device control program that includes system documentation and procedures for managing network devices. Without an effective network device policy, the risk that Systems Division personnel could inconsistently configure or use network devices increases, and therefore, limits the effectiveness of those devices in securing the network. Because a network IDS monitors events and activity occurring on the network, including signs of possible security

(FOUO) incidents, DMDC personnel should develop polic ^{DMDC (b)(5)}
[Redacted]

(FOUO) ^{DMDC (b)(5)}
(FOUO) ^{DMDC (b)(5)}
[Redacted]

(FOUO) ^{DMDC (b)(5)}
[Redacted]

Conclusion

(FOUO) ^{DMDC (b)(5)}
[Redacted]

[Redacted]

⁹ (FOUO) ^{DMDC (b)(5)}
[Redacted]

DMDC (b)(5)

Management Comments on the Finding and Our Response

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed risk management processes and procedures needed improvement; however, the Deputy Director partially agreed security measures were insufficient to identify and protect DEERS from known vulnerabilities, ^{DMDC (b)(5)}

(FOUO) ^{DMDC (b)(5)}

The Deputy Director stated DMDC performed annual vulnerability testing and monthly scans using Retina to confirm the progress and effectiveness of ongoing mitigation actions. The Deputy Director stated DEERS relied heavily on Oracle and pointed out that Oracle released quarterly security patches that DMDC then tested before including them in the next scheduled maintenance update, ^{DMDC (b)(5)}

The Deputy Director also acknowledged DMDC was continuing to evaluate alternative virus protection software and Security Technical Implementation Guide compliance tools to improve overall security.

(FOUO) ^{DMDC (b)(5)}

(FOUO) DMDC (b)(5)
[Redacted]

(FOUO) DMDC (b)(5)
[Redacted]

Our Response

(FOUO) We have addressed each of the issues as presented. We agree DMDC performed annual vulnerability testing on the DEERS operating system, but continue to believe the DEERS operating system was not sufficiently protected. DMDC did not provide documentation supporting its assertions about completing monthly vulnerability scans using Retina. Vulnerability assessments identify weaknesses at a specific point in time when the assessment occurs. DMDC (b)(5)

[Redacted] If DMDC conducted monthly vulnerability assessments to verify its progress and effectiveness in mitigating weaknesses from previous vulnerability assessments, we would expect the plan of action and milestones to contain notations or results concerning those monthly scans to assist DMDC in tracking its progress. The plan of action and milestones DMDC provided did not include those types of details. DoD Instruction 8500.2 control VIVM-1 requires the implementation of a comprehensive and ongoing vulnerability management program that identifies and mitigates vulnerabilities. DMDC monthly vulnerability scans, if performed, should be completed to track the status of mitigation efforts and to continuously identify and mitigate the risk of newly identified vulnerabilities. DMDC (b)(5)

[Redacted]

(FOUO) DMDC (b)(5)
[Redacted]

~~(FOUO)~~ DMDC (b)(5)

~~(FOUO)~~ The Systems Division, specifically the Network Infrastructure branch, was responsible for managing DMDC security devices. DMDC (b)(5)

Additionally, DMDC used VPNs to support internal and external communications; however, only external communications were visible to the network IDS. An IDS inspects activity occurring within a network or specific host to identify suspicious patterns that may indicate an attack from someone attempting compromise a system or network. DMDC used internal VPNs to further improve its overall security posture and protect the PII and other sensitive data processed through DEERS, but minimized the additional protection afforded through the use of VPNs because they were not visible to, or monitored by a network IDS. DoD Instruction 8500.2 control EBVC-1 does not distinguish between internal and external VPN connections when requiring VPN communications to be visible to a network IDS.

Recommendations, Management Comments, and Our Response

A. We recommend that the Director, Defense Manpower Data Center:

1. Update the Defense Manpower Data Center Information Assurance Policy, November 4, 2009, to require:

~~(FOUO)~~ (a) Systems and Technical Support Division personnel 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.

(b) Systems and Technical Support Division personnel formally document and submit the results of periodic vulnerability assessments to the Defense Manpower Data Center Information Systems Security Group to ensure it properly manages known vulnerabilities affecting the agency's information systems.

(c) System owners prepare formal risk assessments that are approved by the Defense Manpower Data Center chief information officer before outsourcing key information assurance services.

(d) Technology Steering Group personnel formally document evaluations that support the risk of using public domain software on Defense Manpower Data Center information systems and that are approved by the Defense Manpower Data Center Designated Accrediting Authority.

DMDC Comments

DMDC (b)(5)
[Redacted]

Our Response

DMDC comments were responsive; however, the comments did not include a completion date for updating the IA Policy. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

(FOUO) 2. DMDC (b)(5)
[Redacted]

DMDC (b)(5)
(FOUO) DMDC (b)(5)
[Redacted]

Our Response

DMDC comments were responsive; however, the comments did not include a completion date for [Redacted]. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

(FOUO) 3. Complete ongoing evaluations to acquire up-to-date [Redacted] Defense Enrollment Eligibility Reporting System servers.

DMDC Comments

(FOUO) The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating DMDC implemented virus protection software and updated virus

(FOUO) protection signatures on all DEERS ^{DMDC (b)(5)}

[REDACTED]

Our Response

(FOUO) DMDC comments were responsive; however, the comments did not include a completion date for developing an automated script to schedule updates. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

(FOUO) ^{DMDC (b)(5)}

[REDACTED]

DMDC Comments

(FOUO) The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating DoD Instruction 8500.2 control ^{DMDC (b)(5)}

[REDACTED]

Our Response

(FOUO) DMDC comments are partially responsive to the intent of our recommendation. We agree DoD Instruction 8500.2 control ^{DMDC (b)(5)}

[REDACTED]

[REDACTED]

(FOUO) DMDC (b)(5) [Redacted]

(FOUO) 5. Perform a review to determine necessary staffing requirements and acquire [Redacted]

DMDC Comments

(FOUO) The Deputy Director, DMDC, [Redacted]

Our Response

(FOUO) DMDC comments were responsive, and proposed actions will address our concerns; however, the comments did not include a completion date for evaluating resources and [Redacted]. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

(FOUO) 6. [Redacted]

DMDC Comments

(FOUO) DMDC (b)(5) [Redacted]

Our Response

(FOUO) DMDC (b)(5) [Redacted]

~~(FOUO)~~ DMDC (b)(5)
[Redacted]

~~(FOUO)~~ DMDC (b)(5)
[Redacted]

DMDC Comments

DMDC (b)(5)
[Redacted]

Our Response

~~(FOUO)~~ DMDC (b)(5)
[Redacted]

8. Develop policy and procedures for managing, configuring, and securing Defense Manpower Data Center network devices.

DMDC Comments

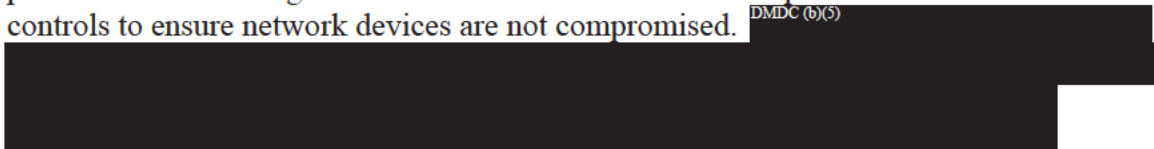
~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating the Systems Division Network Infrastructure branch strictly controlled access to network devices and used Tripwire to verify network device configuration settings. Additionally, the Deputy Director stated DMDC had written standard operating procedures addressing many processes, but acknowledged procedures were not in place for all processes.

Our Response


DMDC comments were nonresponsive to the intent of the recommendation. The DMDC IA Policy briefly describes requirements for submitting change requests when configuring routers and switches and also describes physically securing and maintaining

access to firewalls. Because the policy did not describe how to logically manage access to DMDC security devices, we requested additional documentation. As a result, the Network Infrastructure manager provided the IP and VLAN Standards to further demonstrate how DMDC configured and logically protected access to its security devices. However, those standards merely identify Internet Protocol ranges available to support DMDC security devices and the types of security devices supporting the DMDC security posture.

~~(FOUO)~~ We do not believe the DMDC IA Policy and the IP and VLAN Standards meet the intent of DoD Instruction 8500.2 control ECND-2, which requires the development of procedures for limiting access to network devices and the implementation of technical controls to ensure network devices are not compromised. ^{DMDC (b)(5)}

 Additionally, DMDC did not ensure all VPN communications were properly monitored by a network IDS; external VPN communications were monitored by a network IDS, but internal VPN communications were not. DoD Instruction 8500.2 control EBVC-1 requires all VPN communications to be monitored by a network IDS.

~~(FOUO)~~ We also disagree access to all network security devices were strictly controlled. We identified the security support structure, known as the virtual local area network, ^{DMDC (b)}

 Those weaknesses might not have existed had DMDC policy and procedures been more robust in addressing requirements for managing, configuring, and securing network devices. Therefore, we request the Director, DMDC, reconsider her position about strengthening policy and developing additional procedures, and provide comments on the final report by July 20, 2012.

~~(FOUO)~~ **9. Deploy host-based intrusion detection systems on the 13 Defense Enrollment Eligibility Reporting System production, contingency failover, and test servers not currently protected by these security devices.**

DMDC Comments

~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating DMDC installed Tripwire on the ^{DMDC} DEERS servers, but has only begun actively monitoring activity on ^{DMDC} of those servers because additional network communications are needed to allow for continuous monitoring on the remaining ^{DMDC} servers.

Our Response

~~(FOUO)~~ DMDC comments are responsive, and proposed actions will address our concerns; however, the comments did not include a completion date for actively

(FOUO) monitoring actions occurring on the remaining two servers. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

10. Review the performance of the officials responsible for managing the Defense Manpower Data Center information assurance program, including the Defense Enrollment Eligibility Reporting System security posture, and based on the results consider corrective actions, as appropriate to meet DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, information assurance requirements.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating DMDC appointed a new CIO and IAM and is in the process of revising the IA architecture to provide greater oversight of security operations and separation of duties.

Our Response

DMDC comments were responsive, and proposed actions will address our concerns; however, the comments did not include a completion date for updating the IA architecture. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

Finding B. Stronger Controls Needed to Prevent Unauthorized Access

DMDC (b)(5) [Redacted]

- | [Redacted]
- | [Redacted]
- | [Redacted]
- | [Redacted]

[Redacted]

- | [Redacted]
- | [Redacted]

- (FOUO) DMDC (b)(5) [Redacted]

(FOUO) DMDC (b)(5) [Redacted]

Improvements Needed to Account for Personnel Supporting DEERS

Of the ^{DMDC} IA controls DMDC personnel implemented with deficiencies, ^{DMDC (b)(5)} ^{DMDC (b)(5)}. Personnel in the DEERS and Systems Divisions did not implement adequate internal controls to appropriately account for the ^{DMDC} personnel that they identified as supporting DEERS operations and did not effectively manage access to DEERS applications. The DISSG did not appoint in writing ^{DMDC} SAs and database administrators performing IA roles and responsibilities supporting DEERS operations. In addition, they did not implement a process to ensure required actions were completed during personnel out processing. Further, Systems Division personnel did not include an appropriate contractor affiliation display on ^{DMDC} ^{DMDC} DoD-issued e-mail accounts we reviewed.

Comprehensive Account Management Process Needed

DEERS Division personnel did not implement a comprehensive account management process to accurately account for personnel supporting DEERS operations as required by DoD Instruction 8500.2 control IAAC-1 (Account Control) although contractors primarily supported these operations. This control requires a comprehensive account management process to be implemented to ensure only authorized users can gain access to workstations, applications, and networks. Documentation showed that ^{DMDC} ^{DMDC (b)(5)} supported DEERS operations at DMDC Seaside and SMC Auburn Hills. ^{DMDC (b)(5)}. Accountability of personnel supporting DEERS operations, including those at SMC Auburn Hills and in the DEERS, Enterprise Services, and Systems Divisions at DMDC, was insufficient because DMDC did not maintain an up-to-date master list of personnel supporting specific systems within the organization. For example, the results of the 2009 DMDC continuity of operations test showed that the organization did not have updated personnel listings.

DMDC should fully account for all personnel supporting DEERS operations to ensure access occurs only by authorized personnel with a need-to-know. Without being able to completely account for all personnel supporting DEERS operations and that have access to the system, DMDC limits its ability to verify whether only personnel that have a demonstrated need-to-know could access DEERS servers, databases, and data. Consequently, personnel in the DEERS, Enterprise Services, and Systems Divisions should develop a process to accurately account for, and periodically review personnel with access to the DEERS operating system.

^{DMDC (b)(5)}

Applications Was Not Properly Managed

~~(FOUO)~~ Five application managers responsible for managing ^{DMDC (b)(5)} DEERS applications did not maintain memorandums of understanding for 45 sites and New Site and Site Security Manager Permission Request Forms for ^{DMDC (b)(5)}. Also, the documentation for the remaining ^{DMDC} sites was not always accurate. ^{DMDC (b)(5)}

DoD Instruction 8500.2

~~(FOUO)~~ control IAAC-1 requires system owners to maintain a comprehensive account management process to ensure only authorized users can access applications.

Application managers were responsible for providing access to sites and site security managers for the applications that they managed and for maintaining documentation, including memorandums of understanding and New Site and Site Security Manager Permission Request Forms, to support approved access to those applications. Two DEERS application managers stated that the New Site and Site Security Manager Permission Request Form identified which applications were needed at a site, and established accountability for managing access at the site. However, for ^{DMDC (b)(5)} sites that we reviewed in which DMDC personnel provided documentation, only ^{DMDC} forms accurately identified DEERS applications that were being used and the appropriate site security manager. The remaining forms did not support the site's use of DEERS applications and did not identify the appropriate site security manager accountable for managing access at those sites because the DEERS Division Director did not hold application managers accountable for managing access to DEERS applications.

~~(FOUO)~~ Neither site security managers nor DEERS application managers effectively monitored the status of inactive accounts to ensure they were promptly deactivated as required by DoD Instruction 8500.2 control IAAC-1. Two DEERS application managers stated that site security managers were responsible for verifying eligibility of personnel at their sites, maintaining user access request documentation, and managing inactive user accounts, but written procedures defining these responsibilities did not exist. Therefore, the DEERS Division Director, should develop procedures that hold DEERS application managers and site security managers accountable for managing and controlling access. These procedures should address requirements for maintaining documentation and monitoring account activity to ensure inactive accounts are promptly deactivated. A DEERS Division branch chief stated that site security managers were required to deactivate accounts that were inactive for more than ^{DMDC} days. However, ^{DMDC (b)(5)} user accounts were inactive for more than ^{DMDC} days, of which ^{DMDC (b)(5)} not deactivated. For example, six user accounts were listed as active accounts in DEERS despite those accounts being inactive for at least ^{DMDC (b)} days; one account was inactive for ^{DMDC (b)} days.

~~(FOUO)~~ In addition, the CIO stated that DEERS was designed to automatically deactivate accounts after a period of inactivity. However, evidence from our review shows that those automated settings were not either implemented or properly configured as the CIO had stated. Therefore, the DEERS and Systems Divisions should review existing configuration settings to validate whether the automated functionality to deactivate accounts that are inactive for more than 60 days was properly configured. By not implementing an effective process for managing access to DEERS applications that includes promptly deactivating inactive user accounts using either a manual or automated process, DMDC increased its risk that unauthorized access, modification, or loss of sensitive DEERS data could occur.

IA Appointments Were Not Always in Writing and Roles and Responsibilities Were Not Clearly Defined

The DISSG did not properly appoint in writing ^{DM}_{DC} SAs and database administrators that were designated in IA technical positions supporting DEERS operations. DoD Instruction 8500.2 control DCSD-1 (IA Documentation) requires all appointments to IA roles be established in writing. According to an IAO, DMDC only appointed in writing personnel that perform IA responsibilities as their primary duty in accordance with requirements in DoD 8570.01-M, “Information Assurance Workforce Improvement Program,” April 20, 2010. For example, appointments in writing were completed for the DMDC Designated Accrediting Authority, the Certifying Authority, IAM, and the DEERS IAO. The IAO further stated that although personnel, such as SAs and database administrators, performed IA functions, DISSG did not appoint in writing those personnel because they believed SAs and database administrators performed an operational role that included secondary IA responsibilities. However, the DISSG misinterpreted DoD 8570.01-M requirements because it only distinguishes primary and secondary IA responsibilities for reporting purposes. DoD 8570.01-M explicitly requires personnel designated in IA technical and IA management positions to be appointed in writing. According to documentation, SAs and database administrators were designated in IA technical positions and were therefore required to be appointed in writing. However, those personnel were not appointed in writing.

In addition, appointment letters for three of the four positions that DMDC provided did not always clearly define IA roles and responsibilities. Specifically, those positions were

Without clearly defined responsibilities, personnel in IA positions could potentially misinterpret or perform inappropriate roles and responsibilities.

the certifying official, IAM, and DEERS IAO. The appointments referred the appointees to broad and comprehensive DoD guidance instead of defining specific roles and responsibilities the personnel were expected to perform. Without clearly defined responsibilities, personnel in IA positions could potentially misinterpret or perform inappropriate roles and responsibilities. Therefore, the DISSG should appropriately appoint in writing personnel designated in IA technical and IA management positions.

Actions for Out Processing Personnel Were Not Effective

The DMDC’s out processing procedures were not effective to verify whether Government property was collected, and network and system accounts had been promptly disabled or deactivated for 12 personnel. DoD Instruction 8500.2 control IAAC-1 requires accounts designated as inactive, suspended, or terminated to be promptly deactivated or removed. The DEERS IAO stated that division chiefs were responsible for electronically sending employee action forms that identified the individual and the date of separation to DMDC trusted agents¹⁰ to initiate out processing actions in accordance with

¹⁰ Trusted agents are DMDC personnel responsible for completing all required out processing actions, including collecting government property and removing access to the network or an information system.

the DMDC IA Policy established by the DISSG. Although employee action forms included requirements for out processing personnel, the DMDC's process was decentralized and did not ensure trusted agents documented (audit trail) whether they had completed actions within their areas of responsibility. For example, none of the employee action forms for ^{DM}_{DC} DMDC personnel that out processed since September 17, 2010, included evidence that actions to properly out process those personnel had been performed. However, the DMDC IA Policy requires the use of both an employee action form and an associate termination checklist, which includes further step-by-step procedures for out processing personnel. Despite the requirements, trusted agents did not complete that checklist for any of the ^{DM}_{DC} personnel because they relied solely on the employee action form to out process those personnel. Therefore, the DISSG should establish a centralized function to verify whether trusted agents have properly and promptly completed actions in accordance with existing out processing procedures and documentation requirements in the DMDC IA Policy.

~~(FOUO)~~ In addition, the DMDC Seaside data center manager stated that DMDC used the ^{DM}_{DC} (b)(5) to remove network access based on employee actions forms.

~~(FOUO)~~ We believe 52 days was excessive because a user could potentially access DMDC resources, including DEERS, no longer authorized.

According to ^{DM}_{DC} (b)(5) change requests, trusted agents took between ^{DM}_{DC} (b)(5) days to remove access privileges for the ^{DM}_{DC} personnel that separated from DMDC since September 2010. Although neither DoD Instruction 8500.2 nor National Institute of Standards and Technology Special Publication 800-53 define a period of time for deactivating accounts or removing access privileges, we believe ^{DM}_{DC} days was excessive

because a user could potentially access DMDC resources, including DEERS, no longer authorized. Therefore, the DISSG should define a reasonable period of time for promptly deactivating and removing account access and hold trusted agents accountable for completing actions within that period.

E-Mail Account Designations Did Not Meet DoD Requirements

Systems Division personnel did not configure all contractor e-mail accounts supporting DEERS operations with an appropriate designation. Specifically, domain administrators did not include an appropriate ".ctr" affiliation display in ^{DM}_{DC} (b)(5) accounts as required by DoD Instruction 8500.2 control ECAD-1 (Affiliation Display) because they did not verify whether the content of all contractor e-mail accounts was correct before establishing them in the DoD Global Address List. Although DMDC personnel took action to correct six of the inappropriate network accounts and remove one account because the individual left DMDC, one e-mail account was not corrected. Therefore, domain administrators should configure the remaining contractor e-mail account to include an appropriate ".ctr" affiliation display to prevent an inadvertent disclosure of information to DoD contractors and review whether all contractor e-mail accounts supporting DMDC operations have been appropriately configured.

Access to DEERS and DMDC Network Devices Was Not Effectively Managed

~~(FOUO)~~ Personnel from the DEERS and Systems Divisions did not consistently require personnel with access to the DMDC Seaside data center or the DEERS operating system and Oracle databases to complete written authorization request forms before accessing those resources. DEERS Division personnel also did not effectively manage the process for sharing DEERS data with DoD, Federal, and State agencies. In addition, Systems Division personnel inconsistently managed access to DMDC resources that could allow remote access to critical files and data within the DEERS operating system. Further, a contracting officer's representative in the Business Operations and Management Division did not verify whether SMC Auburn Hills personnel supporting DEERS had completed appropriate security training.

Access to the DMDC Seaside Data Center Was Not Documented

Systems Division personnel did not maintain appropriate documentation supporting whether all personnel were approved in writing to access the DMDC Seaside data center. Specifically, the DMDC Seaside data center manager did not maintain a DMDC User Agreement for all ^{DM}_{DC} personnel included on the data center's access roster. DoD Instruction 8500.2 control PECF-1 (Access to Computing Facilities) requires only authorized personnel with a need-to-know to be granted physical access to computing facilities that process sensitive information. The Data Center Entrance and Exit Procedures, May 13, 2009, define processes and responsibilities for maintaining security over the DMDC Seaside data center. However, that documentation did not describe procedures for granting access to the data center. The data center manager stated that he only maintained agreements signed after he became the data center manager in July 2008, but granted all other personnel access by "grandfathering" them in place without formal documentation establishing their need-to-know.

The data center manager did not validate whether the ^{DM}_{DC} personnel with access to the data center had a current DMDC User Agreement on file because he did not make it a priority. By not ensuring all personnel signed DMDC User Agreements, the data center manager decreases his ability to effectively manage access to a controlled area. Therefore, the Systems Division data center manager should annually validate whether personnel with access to the DMDC Seaside data center still require access to that facility and require them to complete a DMDC User Agreement.

Documentation Did Not Exist to Support the Need for Access

~~(FOUO)~~ Systems Division personnel could not identify all DMDC Seaside and SMC Auburn Hills personnel with access to ^{DMDC}_(b) DEERS servers and did not provide evidence supporting whether personnel received access to DEERS system hardware and Oracle databases based on an approved written authorization request form. Specifically, they did not verify whether appropriate documentation was properly completed or maintained for

~~(FOUO)~~ all personnel with privileged¹¹ and non-privileged access to Unix servers or Oracle databases. DoD Instruction 8500.2 control IAAC-1 requires a comprehensive account management process to be implemented to ensure only authorized users access workstations, applications, and networks. In addition, National Institute of Standards and Technology Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” May 1, 2010, requires access to be granted based on a valid access authorization.¹²

~~(FOUO)~~ Although DMDC established procedures requiring the use of a Unix Project Accounts Action Form or an Oracle Account Action Form when requesting access, Systems Division personnel provided documentation for only one SA although we

~~(FOUO)~~ Directors of the DEERS and Enterprise Services Divisions stated that although the DMDC IA Policy requires access to be reviewed on a regular basis, they did not revalidate access to DEERS servers, Oracle databases, and production code . . .

requested documentation for all personnel with access to ~~(FOUO)~~ DEERS servers. Because DMDC updated (refreshed) DEERS servers within the past ~~(FOUO)~~, the DMDC Seaside data center manager stated that written authorization requests should have been completed. However, the Directors of the DEERS and Enterprise Services Divisions stated that although the DMDC IA Policy requires access to be reviewed

on a regular basis, they did not revalidate access to DEERS servers, Oracle databases, and production code because they believed such actions were not necessary since their personnel generally stayed in the same positions and their duties did not change. DoD Instruction 8500.2 control ECPC-2 (Production Code Change Controls) requires access to production code to be revalidated every 3 months.

~~(FOUO)~~ Without a complete and thorough audit trail that demonstrates whether personnel had been granted privileged access based on approved authorization request forms, the Systems Division limits its ability to verify whether only authorized personnel obtain access to DEERS system hardware and Oracle databases. In addition, the Systems Division decreases its ability to ensure the need for access remains by not revalidating access. As such, DMDC should perform a reconciliation of its personnel with access to DEERS servers and Oracle databases to verify whether the need for access remains, and then periodically, at least annually, revalidate access.

~~(FOUO)~~ In addition, the process did not sufficiently demonstrate that access had been granted based on need-to-know or the principle of least privilege. DoD Instruction 8500.2 control ECAN-1 (Access for Need-to-Know) requires access to all DoD information to be determined by a user’s need-to-know. The DMDC IA Policy also requires access to DMDC information systems to be based on the principle of least privilege and granted solely to personnel who have a justifiable need. Information in the justification section of the Unix Project Accounts Action Form or Oracle Account Action

¹¹ DMDC refers to privileged access as elevated access and non-privileged access as authorized access.

¹² National Institute of Standards and Technology Special Publication 800-53 control AC-2 requires written access authorization requests.

~~(FOUO)~~ Form represented the users need-to-know; however, documentation provided by Systems Division personnel did not clearly demonstrate an operational business case (justification). For example, the only Unix Project Accounts Action Form provided did not include any information in the justification section even though the SA had requested privileged access to all DEERS servers.

~~(FOUO)~~ Further, documentation did not include a sufficient audit trail to support whether personnel from the DEERS and Systems Divisions granted access based on the principle of least privilege. DoD Instruction 8500.2 controls ECLP-1 (Least Privilege) and PRNK-1 (Access to Need-to-Know Information) require access to privileged accounts to be limited to privileged users that meet all personnel security requirements. However, neither the Unix Project Accounts Action Form nor the Oracle Account Action Form required personnel to document whether the requestor had been appropriately cleared (vetted). Personnel in the DEERS and Systems Divisions responsible for approving access did not verify whether the requestor had an appropriate security clearance commensurate with assigned responsibilities, especially when those responsibilities resulted in increased responsibility or additional access privileges. Although an IAO stated that personnel at DMDC Seaside were initially vetted at a minimum of an Information Technology-II level clearance, some positions and responsibilities required an Information Technology-I level clearance, which involves more stringent vetting procedures. Without the structure and formality of documenting repeatable functions and processes, such as demonstrating need-to-know and least privilege, DMDC lacked an effective foundation for ensuring only authorized personnel accessed the DEERS operating system. Therefore, DMDC should update existing procedures to ensure access to the DEERS operating system and Oracle databases is granted based on a valid need-to-know and the principle of least privilege.

Data Sharing Agreements Were Not Always Provided and Were Inconsistently Managed

DMDC (b)(5)



DoD Instruction 8500.2 control DCID-1 (Interconnection Documentation) requires documentation that supports the coordination and exchange of connection rules and requirements to be maintained. In addition, the National Institute of Standards and Technology Special Publication 800-47, "Security Guide for Interconnecting Information Technology System," August 2002, 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.

A memorandum of agreement specifies key information about an interface such as impacted parties, interconnection requirements, points of contact, security requirements, technical platform information, interface file information, and designated signatories. In addition, a memorandum of agreement establishes requirements and organizational

responsibilities to facilitate the accurate and timely transfer of data between systems. Although DMDC officials used memorandums of agreement to document and to establish accountability for the disposition and sharing of DEERS data, ^{DMDC (b)(5)}

[REDACTED]

[REDACTED]

Remote Access to DMDC Resources Was Inconsistently Approved and Managed

Although the DMDC IA Policy defines a process for granting remote access, Systems Division personnel did not follow those procedures. Specifically, they inconsistently approved remote access and did not regularly revalidate the need for personnel to retain remote access accounts. The User Support Services manager stated that all personnel were required to complete a remote access request form, and obtain approval by their division chief before the Systems Division granted them remote access. However, documentation supported that remote access had been approved for only ^{DMDC (b)(5)} DMDC personnel we reviewed. In addition, the User Support Services manager could not provide documentation to support remote access approval for the ^{DMDC} SMC Auburn Hills personnel we reviewed.

~~(FOUO)~~ Although a remote access request form was required, Systems Division personnel did not consistently manage this process because they accepted wide-ranging documentation, such as employee action forms, software and system hardware request forms, and e-mails as support for remote access. In addition, we originally found two other DMDC Seaside personnel had remote access even though documentation showed that their remote access accounts expired as far back as May 2008. However, Systems Division personnel did not revalidate the continued need for remote access. In general, DMDC personnel did not revalidate access to DMDC resources because they believed such actions were not necessary since personnel generally stayed in the same positions and their duties did not change even though the DMDC IA Policy requires remote access

accounts to be reviewed at least annually. Therefore, Systems Division personnel should consistently manage the process for granting remote access and periodically (at least annually) revalidate the continued need for this type of access.

Contractors at SMC Auburn Hills Did Not Complete Annual Security Awareness Training

~~(FOUO)~~ SMC Auburn Hills personnel retained access to DEERS system hardware without completing security awareness training. DoD Instruction 8500.2 control PRTN-1

However, none of the ^{DM}_{DC} SMC Auburn Hills personnel completed annual security awareness training since the DISSG initially approved those personnel to support DMDC operations as far back as October 2008.

(Information Assurance Training) requires all personnel to complete security awareness training to perform their assigned IA responsibilities upon arrival, and periodically thereafter. In addition, contract HC1028-08-D-2018 with Hewlett Packard requires SMC Auburn Hills personnel to complete annual security awareness training. However, none of the ^{DM}_{DC} SMC Auburn Hills personnel completed annual security awareness training since the DISSG

initially approved those personnel to support DMDC operations as far back as October 2008. According to a technical consultant (contractor) at SMC Auburn Hills, SMC Auburn Hills personnel only completed annual Privacy Act training because they were unaware of requirements to take annual security awareness training.

The DMDC IA Policy requires all users of DMDC resources to complete security awareness refresher training at least annually. DISSG information technology specialists stated that they verified whether all Government and contractor personnel at DMDC Seaside completed annual security awareness training requirements. However, they did not validate whether SMC Auburn Hills personnel completed annual training requirements because those ^{DM}_{DC} personnel did not have DoD e-mail accounts. Although SMC personnel did not have DoD e-mail accounts, the contract still required them to complete annual security awareness training. The SMC Auburn Hills technical consultant (contractor) stated that although he had a DoD e-mail account from DMDC, he did not use it because the Hewlett Packard network at SMC Auburn Hills did not support encrypted e-mails.

~~(FOUO)~~ In addition, the contracting officer's representative from the Business Operations and Management Division did not provide effective oversight of the contract to verify whether all contractual requirements, including annual security awareness training, were met. According to the contracting officer's representative, she only oversaw financial matters pertaining to the contract. She stated that Systems Division personnel were responsible for overseeing the completion of all technical compliance matters associated with the contract. However, the contracting officer's representative appointment letter restricts her from further delegating responsibilities. The contracting officer's representative appointment letter, which she signed, explicitly requires her to verify whether the contractor complies with all contractual requirements and perform effective and proactive technical monitoring and administrative oversight of the contractor's work. By not verifying whether all requirements of the contract were met,

(FOUO) the contracting officer's representative did not ensure SMC Auburn Hills personnel were aware of, and adhered to, standards of conduct necessary to protect sensitive information processed by DEERS. Therefore, the DMDC Director, in coordination with the contracting officer, should review her performance related to overseeing contract HC1028-08-D-2018 and based on the results consider corrective actions, as appropriate to ensure all contractual requirements are met.

Additional Protection Needed for the DMDC Seaside Data Center

(FOUO) Although DISSG and Systems Division personnel implemented physical security over DoD Center Monterey Bay and the data center hosting the DMDC DEERS contingency failover, test, and production servers, they did not fully secure all external points of access to the data center. DoD Instruction 8500.2 control PEPF-1 (Physical Protection of Facilities) requires all physical access points to facilities processing sensitive information to be controlled during working hours and secured during non-work hours. Physical security measures used to protect the data center include internal motion detectors, perimeter cameras, Federal police, and a door alarm system; however, none of them directly protected entry to the data center DMDC (b)(5). The DMDC Seaside data center was located DMDC (b)(5).

DMDC (b)(5) Figures 2 and 3 show the exterior of the data center at DoD Center Monterey Bay.

(FOUO) Figure 2.

DMDC (b)(5)

(FOUO) Figure 3.

DMDC (b)(5)

DMDC (b)(5)

Source: DoD Office of Inspector General

(FOUO) DMDC (b)(5)

Conclusion

(FOUO) DMDC personnel did not implement a comprehensive process for managing and controlling access to DEERS data and its operating system, including Unix servers and Oracle databases. Specifically, DMDC’s processes and procedures were insufficient to ensure that only authorized personnel with a valid need-to-know were granted access to DEERS and its sensitive data, which includes PII for approximately 37 million military personnel and retirees, their families, DoD civilians, and contractors. In general, DMDC officials did not ^{DMDC (b)(5)} [REDACTED], periodically revalidate the continued need for access, and promptly remove or deactivate inactive accounts. Although we did not identify any instances in which DEERS data had been compromised, the necessity for repeatable and effective access controls is essential to providing integrated, layered protection of DEERS data and its operating system. To effectively withstand internal and external cyber attacks, DMDC officials must ensure they have stringent operational access controls in place.

Management Comments on the Finding and Our Response

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed DMDC needed additional protection to protect the DMDC Seaside data center, but partially agreed improvements were needed to account for personnel supporting DEERS operations. Specifically, the Deputy Director stated the Systems Division SAs and database administrators provided services for all DMDC systems, including DEERS, but also indicated specific projects may be assigned specific database administrators with lesser privileges. The Deputy Director also acknowledged DMDC SAs and database administrators were not appointed in writing.

In addition, the Deputy Director stated the DMDC IA Policy requires system privileges to be revoked for all out processed personnel and indicated the DEERS IAO maintained a list of all DEERS personnel for the purpose of ensuring system privileges and accounts were properly revoked. The Deputy Director stated “the DoD OIG’s assertion was

largely based on the existence of a tickler checklist for out-processing in the DMDC IA Policy,” which they did not retain. The Deputy Director stated a DMDC security officer recently completed an audit of 15 personnel that separated from DMDC to ensure access privileges had been revoked; the results of that assessment found physical and logical access had been properly revoked. Additionally, the Deputy Director stated DMDC would begin documenting audits to evaluate whether out processed personnel access privileges were properly revoked as a means of complying with policy. Further, the Deputy Director stated DMDC required contractor e-mail addresses to include a “.ctr” affiliation display and also indicated the eight contractor e-mail addresses we cited were correct. However, the Deputy Director also acknowledged those same accounts had an incorrect alias.

~~(FOUO)~~ The Deputy Director disagreed DMDC did not effectively manage access to DEERS and DMDC network devices. The Deputy Director stated the Systems Division, specifically the Network Infrastructure branch, controlled access to DMDC network devices and only allowed a small number of system administrators access to those devices. The Deputy Director further stated DMDC used Tripwire to verify the configuration of all network devices.

Our Response

We agree SAs and database administrators were generally not assigned to specific systems, such as DEERS; rather, they supported overall DMDC operations. However, DoD 8570.01-M requires all personnel performing IA responsibilities, regardless of whether they support enterprise operations or specific systems, to be appointed in writing with clearly defined roles and responsibilities.

~~(FOUO)~~ We disagree with the Deputy Director’s opinion that we largely based our conclusions on the absence of associate termination checklists. Our conclusions on DMDC out processing actions were based on discussions with the DEERS IAO and Systems Division personnel and reviewing the DMDC IA Policy, an ad-hoc spreadsheet of DEERS Division personnel maintained by the DEERS IAO, employee action forms, and ^{DMDC (b)(5)} [REDACTED]. Although the DMDC IA Policy explicitly requires the Chiefs of the Operations and Systems Divisions to promptly revoke physical and logical access to DMDC resources, documentation from the ^{DMDC (b)(5)} [REDACTED] showed trusted agents took between ^{DMDC (b)(5)} [REDACTED] days to remove network access for ^{DMDC (b)(5)} [REDACTED] personnel that separated from DMDC since September 17, 2010. Despite DMDC personnel revoking access, we do not believe ^{DMDC (b)(5)} [REDACTED] is a reasonable period for removing access to the DMDC network because that period of delay could allow personnel time to use existing knowledge of DMDC operations to access resources no longer authorized. We agree audits of actions taken to out process personnel could provide DMDC assurance that required actions have been properly taken, and commend DMDC for beginning this process. However, we continue to believe DMDC also need to establish a reasonable period of time for revoking logical and physical access to all DMDC resources.

Although the Deputy Director stated “the Network branch of the Systems Division strictly controls all access to network devices,” we disagree. The DMDC comments primarily addressed physical access to DMDC network security devices, but the report discussed broader issues. Overall, DMDC did not have an effective process in place for substantiating whether personnel with access to the DMDC Seaside data center and therefore, system hardware, were approved access based on demonstrated operational requirements and a legitimate need for access to that area. While we do not believe they allowed everyone access to controlled areas, documentation did not support the need for access. Additionally, documentation did not substantiate the need for privileged access to DMDC system hardware and software supporting DEERS operations and the operational need for remote access to DMDC resources. However, if DMDC implements a more robust process for managing access that includes documentation supporting an operational need and supervisor approval, we believe DMDC controls for managing access will improve. Further, DMDC did not ensure data sharing agreements were always in place with all organizations that interconnected with and had access to DEERS data. Also, the documented agreements generally did not clearly describe the terms and conditions for sharing data in a secure manner.

Recommendations, Management Comments, and Our Response

Revised and Renumbered Recommendations

As a result of management comments, we revised draft Recommendation B.1.a to clarify our intent was to account for personnel with logical access to DEERS servers and databases, B.1.b to account for newly provided documentation, and B.1.f to clarify our intent was to define a reasonable period of time for removing and deactivating access to the DMDC network. We request that the Director, DMDC, provide comments on the final report by July 20, 2012.

B.1. We recommend that the Director, Defense Manpower Data Center:

a. Develop a process to accurately account for, and periodically review, at least annually, Defense Manpower Data Center and Service Management Center Auburn Hills personnel with logical access to the Defense Enrollment Eligibility Reporting System operating system.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating processes existed for managing access to the DMDC Seaside data center. Although the Deputy Director stated SMC Auburn Hills implemented access procedures, DMDC had limited visibility over those processes and would therefore develop a process to manage and account for personnel with access to DMDC system hardware at SMC Auburn Hills.

Our Response

DMDC comments were partially responsive to the intent of our recommendation. Although DMDC agreed to develop a process to account for personnel with physical access to DMDC equipment, specifically DEERS, at SMC Auburn Hills, the intent of our recommendation was to account for personnel with logical access to DEERS servers and databases at DMDC and at SMC Auburn Hills. Therefore, we revised the recommendation to clarify our intent. We request the Director, DMDC, reconsider her position and develop an overall process that accounts for all DMDC and SMC Auburn Hills personnel with logical access to DEERS servers and databases, regardless of which division they are organizationally aligned at DMDC, and provide comments on the final report by July 20, 2012.

b. Update the Guide to Application Security Management, DMDC (b)(5), DMDC (b)(5), for granting access to the Defense Enrollment Eligibility Reporting System applications to specify documentation requirements for a site to obtain access those applications, to include application managers and site security managers responsibilities for maintaining and periodically reviewing the documentation to support whether site access had been properly authorized.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating DMDC issued the Guide to Application Security Management 7 years ago that requires site security managers to review user activity at least monthly and remove accounts no longer requiring access to DEERS applications. Additionally, the Deputy Director stated site security managers were responsible for managing user access at their sites while DMDC was responsible for managing site security manager access. The Deputy Director also acknowledged DMDC did not regularly review the documentation they maintained for site security managers, but would determine appropriate periodic audit requirements.

Our Response

DMDC comments were partially responsive to the intent of our recommendation. We were unaware of the Guide to Application Security Management and were not provided that document during the audit despite requesting procedures that governed the application management process. The Guide to Application Security Management partially addresses our concerns and therefore, we revised the recommendation to account for the newly provided information. The procedures described roles and responsibilities for DEERS application managers and site security managers, including completing a New Site and Site Security Manager Permission Request Form for obtaining access to DEERS applications and managing and monitoring access to DEERS applications.

DEERS application managers stated DMDC required specific documentation to establish access to DEERS applications; however, those requirements were not fully defined in the Guide to Application Security Management and DMDC application managers did not effectively manage those documentation requirements. Specifically, a DEERS

application manager stated DMDC required a justification letter, a New Site and Site Security Manager Permission Request Form, memorandums of understanding, and an authority to operate from the site before approving DEERS access to the site. The Guide to Application Security Management does not address requirements for obtaining or maintaining memorandums of understanding and the authority to operate. DMDC personnel did not maintain memorandums of agreement for any of the ^{DM}_{DC} sites using DEERS applications and could only provide New Site and Site Security Manager Permission Request Forms for ^{DMDC (b)(5)} sites we reviewed. Of the ^{DM}_{DC} New Site and Site Security Manager Permission Request Forms obtained, ^{DMDC (b)(5)} accurately described the applications used at the site and the current site security manager. During the audit, DEERS application managers discussed plans to begin implementing and requiring DD Form 2875 (System Access Authorization Request) for site security managers, but that process had not been finalized.

Although the Guide to Application Security Management partially addresses our concerns for managing DEERS application access at user sites, it was not consistent with the requirements two DEERS application managers stated were currently in place at DMDC. Therefore, we request the Director, DMDC, reconsider her position and update existing processes to define specific roles and responsibilities and documentation requirements, and provide comments on the final report by July 20, 2012.

~~(FOUO)~~ c. **Review configuration settings to validate whether the automated functionality for deactivating accounts inactive for more than 60 days was properly configured and update automated system settings designed to control access to Defense Enrollment Eligibility Reporting System applications to ensure inactive accounts are promptly deactivated.**

DMDC Comments

~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating procedures will be revised to enforce automated suspension of accounts after 60 days of inactivity. The Deputy Director also stated he did not believe we clearly understood the DMDC's use of suspended accounts. The Deputy Director stated DMDC first suspended accounts and then deactivated them if they continued to be inactive for an additional 120 days from the time they were suspended.

Our Response

~~(FOUO)~~ DMDC comments were responsive; however, the comments did not include a completion date for revising procedures ^{DMDC (b)(5)}. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

d. Appoint, in writing, system administrators, database administrators, and other Defense Manpower Data Center personnel performing information assurance roles and responsibilities in accordance with requirements in DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003, and DoD 8570.01-M, “Information Assurance Workforce Improvement Program,” April 20, 2010.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating SAs and database administrators are appointed in writing for some applications and databases, but will appoint, in writing, SAs and database administrators for all systems either by system or at the enterprise level.

Our Response

DMDC comments were responsive; however, the comments did not include a completion date for appointing, in writing, personnel performing IA responsibilities. Therefore, we request the Director, DMDC, provide the completion date for the planned actions.

e. Comply with existing out processing procedures and documentation requirements defined in the Defense Manpower Data Center Information Assurance Policy, November 4, 2009, and establish a centralized function to validate whether required actions have been properly taken.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, disagreed stating the DEERS IAO maintains a list of all DEERS personnel and ensures account privileges are removed when personnel leave DMDC. The Deputy Director also stated he believed our assertion was based largely on the lack of associate employee checklists. The Deputy Director further stated a security officer randomly selected 15 personnel that left DMDC to determine whether access privileges were revoked; the review found physical and logical access had been properly revoked. Additionally, the Deputy Director stated DMDC will begin documenting audits to determine whether access was revoked.

Our Response

DMDC comments were partially responsive to the intent of our recommendation, but assumed we based our conclusion on the lack of associate termination checklists. Our conclusion was based on discussions with the DEERS IAO and our review of DMDC IA Policy requirements and employee action forms for ^{DM}_{DC} personnel that left DMDC as early as September 17, 2010. The DEERS IAO stated she maintained an ad hoc spreadsheet listing personnel with access to DEERS and took it upon herself to annotate actions taken to remove access when personnel separated or were terminated. However, the DEERS IAO also acknowledged she did not always keep her spreadsheet up-to-date. For example, of the ^{DM}_{DC} personnel that left DMDC, the DEERS IAO spreadsheet only showed

access was revoked for ^D_M personnel. According to the DMDC IA Policy, the employee action form and the associate termination checklist were both required to support actions taken by DMDC trusted agents to remove physical and logical access privileges. We agree DMDC maintained employee action forms, but these were not completed to show all actions taken during personnel out processing, to include removing logical and physical access to DEERS.

Although the DEERS IAO attempted to maintain a list of personnel within the DEERS Division, we do not believe the list accounted for all personnel with access to DEERS. During our attempts to identify personnel with logical access to DEERS, DMDC could not provide a single list that accurately identified all personnel. Specifically, personnel outside the DEERS division, including SAs, database administrators, and other personnel performing configuration management duties, had logical access to the system because they also supported DEERS operations. The November 2010 DMDC Seaside reorganization resulted in functions once part of the DEERS Division being moved to other DMDC divisions. Therefore, under the existing DMDC process, personnel in other divisions were not included in the DEERS IAO spreadsheet.

We commend DMDC for implementing a process to audit whether access was revoked; however, we still believe DMDC needs to maintain a sufficient audit trail demonstrating all required out processing actions were promptly completed. We request the Director, DMDC, reconsider her position to maintain relevant documentation required in the DMDC IA Policy that supports actions taken by trusted agents and establish a centralized function to ensure all out processing actions have been taken and provide comments on the final report by July 20, 2012.

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.

DMDC Comments

The Deputy Director, DMDC, responded on behalf of the Director, DMDC, disagreed stating DMDC terminates access by suspending accounts to allow infrequent, but authorized user's accounts, to be reinstated without creating new accounts. The Deputy Director also stated DMDC will develop a process to periodically review active accounts.

Our Response

~~(FOUO)~~ DMDC comments were nonresponsive to the intent of our recommendation because they appear to address issues related to deactivating DEERS application accounts. However, the intent of our recommendation was to develop a reasonable period of time to deactivate and remove access to the DMDC network. As a result, we revised the draft recommendation to clarify our intent. Of the 12 personnel that separated from DMDC since September 17, 2010, ^{DMDC (b)(5)} change requests showed trusted agents took between 2 and 52 days to remove access privileges. We believe 52 days was excessive because a user could potentially access DMDC resources, including DEERS, no longer authorized. Therefore, we request the Director, DMDC,

(FOUO) reconsider her position to develop a reasonable period of time for promptly deactivating and removing access to the DMDC network and provide comments on the final report by July 20, 2012.

g. Review existing contractor e-mail accounts to verify whether they have been properly configured to include a “.ctr” affiliation display.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating the eight e-mail accounts without an appropriate affiliation display were corrected. The Deputy Director also stated DMDC was implementing a process to periodically review all contractor e-mail accounts.

Our Response

DMDC (b)(5)



h. Reconcile and periodically, at least annually, revalidate whether personnel with access to the Defense Manpower Data Center Seaside data center continue to need access to that facility, and require them to complete a Defense Manpower Data Center User Agreement.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating DMDC will evaluate the feasibility of reviewing access control lists to the DMDC Seaside data center and adding additional requirements for annually renewing access to the facilities housing DEERS system hardware. The Deputy Director also stated the DMDC Seaside data center hosts several other tenant organizations.

Our Response

DMDC comments were partially responsive to the intent of our recommendation. Although we were unaware the DMDC Seaside data center hosted other organization's system hardware, those actions did not preclude DMDC from requiring all personnel with access to its computing center to complete the DMDC User Agreement that substantiates an operational justification for accessing a sensitive and controlled area. Additionally, hosting other organizations did not alleviate DMDC from its responsibilities to ensure only authorized personnel were granted physical access to computing facilities in accordance with DoD Instruction 8500.2 control PECF-1. Therefore, we request the Director, DMDC, further consider her position and require all personnel with physical access to the DMDC Seaside data center to be approved in writing, and provide comments on the final report by July 20, 2012.

i. Review and periodically, at least annually, revalidate existing accounts for Defense Manpower Data Center and Service Management Center Auburn Hills personnel with physical and logical access to Defense Enrollment Eligibility Reporting System servers and databases, and reconcile those accounts to verify whether access was granted based on approved user access request forms.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating physical access to all DEERS servers was limited because they resided in data centers. The Deputy Director stated DMDC would develop procedures for reviewing logical access to DEERS servers.

Our Response

~~(FOUO)~~ DMDC comments are partially responsive to the intent of our recommendation. While we agree the Systems Division developed standard operating procedures, “Data Center Entrance and Exit Procedure,” for achieving and maintaining physical security over the DMDC Seaside data center, neither those procedures nor DMDC IA Policy specifically address requirements for periodically revalidating the continued need for physical access to the DEERS operating system. The DMDC Seaside data center manager stated he did not revalidate whether personnel had a continued need to physically access the data center. Additionally, SMC Auburn Hills implements procedures in the Hewlett Packard Global Security Physical Security Process, March 2011, to control physical access to the data center housing the DEERS production environment. The SMC Auburn Hills process of controlling physical access also included quarterly reviews to determine whether personnel should continue to retain physical access to the data center. To ensure only personnel with an authorized and operational need access the DMDC Seaside data center, DMDC should also implement, at a minimum, an annual review process.

~~(FOUO)~~ Although DMDC required personnel requesting logical access to DEERS servers and databases to complete a Unix Project Accounts Action Form or an Oracle Account Action Form, DMDC personnel did not further review whether the operational need for continued access. National Institute of Standards and Technology Special Publication 800-53 requires management to periodically review accounts. Therefore, we request the Director, DMDC, reconsider her position of developing procedures that only include reviewing logical access to DEERS system hardware and develop overall procedures that include periodically reviewing both physical and logical access to DEERS servers and databases, and provide comments on the final report by July 20, 2012.

j. Revise and update existing procedures for granting access to Defense Manpower Data Center systems and resources, to include remote access, that address requirements for:

- (1) periodically revalidating the continued need for access;**
- (2) supervisory review and documented approval of access; and**
- (3) justifying the need and level of access requested.**

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating DMDC will develop processes for periodically reviewing access. However, the Deputy Director also stated procedures were in place for justifying and granting remote access.

Our Response

DMDC comments were partially responsive to the intent of our recommendation. We agree DMDC had procedures for requesting and approving access to DEERS system hardware and software and DMDC resources, including remote access. However, those procedures did not always specifically require the inclusion of an operational business case (justification), supervisory review and approval, and periodic revalidation of the continued need for access. While attempting to determine whether personnel complied with DMDC policies and procedures, we found documentation did not exist, was not complete and accurate, and was not approved because existing procedures did not specifically address these requirements. Therefore, we request the Director, DMDC, reconsider her position and update existing DMDC procedures, and provide comments on the final report by July 20, 2012.

k. ^{DMDC (b)(5)}

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, ^{DMDC (b)(5)}

Our Response

DMDC comments were responsive; ^{DMDC (b)(5)}


~~(FOUO)~~ **1. Implement appropriate security measures to fully protect unsecured access points to the DoD Center Monterey Bay data center.**

DMDC Comments

~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed stating DMDC will implement motion and glass breakage detectors on the windows, as well as physical barriers on the windows that are structurally attached to the building. DMDC expected to implement additional physical safeguards by the end of April 2012.

Our Response

DMDC comments were responsive; therefore, no further comments are required. We contacted DMDC for an update on the status of their actions. The CIO stated DMDC installed and activated the ^{DMDC (b)(5)}



~~(FOUO)~~ **B.2. We recommend the Director, Defense Manpower Data Center, 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.**

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, agreed with the recommendation.

Our Response

DMDC comments were nonresponsive to the intent of our recommendation. Although the Deputy Director agreed with the recommendation, planned actions and the completion date for corrective actions were not provided. Therefore, we request that the Director, DMDC, provide comments on the final report by July 20, 2012.

Finding C. Weaknesses Existed in DEERS Configuration Management Practices

DMDC (b)(5)

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

Security Assessments Were Not Documented

Of the 33 IA controls DMDC implemented with deficiencies, 6 IA controls did not adequately support the security design and configuration of DEERS. The Development Steering Group could not substantiate whether 1,162 software application and 129 system hardware configuration management changes impacted the DEERS security posture. DoD Instruction 8500.2 control DCII-1 (IA Impact Assessment) requires that changes to DoD information systems be assessed for IA and accreditation impact prior to implementation. Although the Development Steering Group Charter, November 17, 2006, and the DEERS Configuration Management Plan, January 2009, requires the Development Steering Group to record meeting minutes when it makes security-related recommendations and evaluations, their deliberations supporting the DEERS security posture were not documented. The IAM stated that DMDC generally relied on program manager's notes to support these types of key decisions; however, DEERS Division personnel either did not maintain that type of documentation or they did not provide it. In addition, Systems Division personnel did not design the Change Management System

██████████ DMDC (b)(5) ¹³ to include information that described whether the IA impact on application and system hardware changes had been properly assessed. The DMDC Organizational Configuration Management Plan, January 2009, states that configuration management is a process that establishes and maintains the security, integrity, and audit capability of an information system.

Without evidence supporting that the required evaluations occurred, DMDC personnel could not substantiate that they had properly assessed all changes before implementing

Without evidence supporting that the required evaluations occurred, DMDC personnel could not substantiate that they had properly assessed all changes before implementing them in the production environment.

them in the production environment. Because the ability to manage changes to an established baseline in a secure manner is hallmark to any successful risk management program, Systems Division personnel must complete and document all security impact evaluations as part of the configuration management process. The documentation should capture the historical

record of management’s decision making process and rationale for making changes that could impact the entire DEERS operating environment.

In addition, the IAM was not directly involved in the DEERS application or system hardware configuration management process as part of either CCB.

DoD Instruction 8500.2 control DCCB-2 (Control Board) requires the IAM to be a member of that board. The IAM stated that he was not a member of either CCB because he had delegated this authority to the DEERS IAO; however, that delegation was not in writing. Further, the IAO was not specifically defined as a member of either CCB. Therefore, the IAM or his designee needs to be an active member having specific and written authority on both CCB.

System Hardware Changes Were Not Always Tested

Systems Division personnel did not test all 129 DEERS system hardware changes that occurred in FY 2010 before implementing those changes in the production environment. Specifically, of the 33 DEERS system hardware changes that we reviewed, DMDC personnel did not test 29, but implemented 25 of those changes in the production environment. DoD Instruction 8500.2 control DCCT-1 (Compliance Testing) requires comprehensive procedures to test all patches, upgrades, and new applications before deployment. According to the system hardware CCB Chair, DEERS system hardware changes were only tested if the Technical Review Board or the CCB recommended testing instead of requiring all changes to be tested.

¹³ DMDC used the Change Management System and ██████████ DMDC (b)(5) as repositories to document the history of management decisions affecting application and system hardware changes, respectively.

By not testing all changes before implementing them in the production environment,

By not testing all changes before implementing them . . . personnel could inadvertently introduce new vulnerabilities not protected by existing IA controls, and therefore, degrade the overall DEERS security posture.

Systems Division personnel could inadvertently introduce new vulnerabilities not protected by existing IA controls, and therefore, degrade the overall DEERS security posture. Therefore, they

should properly test all configuration changes before implementing them in the DEERS production environment.

System Hardware and Software Supporting DEERS Was Not Easily Identifiable

Personnel from the DEERS and Systems Divisions did not maintain a comprehensive baseline of DEERS system hardware and software. DoD Instruction 8500.2 controls DCHW-1 (Hardware Baseline) and DCSW-1 (Software Baseline) require a current and comprehensive baseline inventory of all hardware and software to be maintained. Instead, the Systems Division maintained an enterprise-wide repository of DMDC system hardware in the Configuration Management Database.¹⁴ In addition, the Systems Division separately maintained a Deployable Technology List that included enterprise-wide software supporting DMDC systems. DMDC personnel did not maintain system-specific configuration baselines because they believed the information in the enterprise-wide repositories was sufficient to account for system hardware or software supporting their operations. However, none of the repositories included sufficient details to specifically identify which system the hardware or software supported.

~~(FOUO)~~ For example, Systems Division personnel needed to review the Configuration Management Database and compare the information against other sources to provide us an inventory of DEERS system hardware. During the October 2010 independent contractor IA testing process, DMDC personnel provided an inaccurate baseline of DEERS servers to be tested. Specifically, they identified only ^{DM}_{DC} contingency failover, test, and production servers at DMDC Seaside; however, test results showed ^{DM}_{DC} servers supporting DEERS operations. DMDC's inaccuracies further demonstrate the need to specifically maintain a baseline of DEERS system-specific hardware.

DMDC's inaccuracies further demonstrate the need to specifically maintain a baseline of DEERS system-specific hardware.

Without maintaining a comprehensive baseline of DEERS-specific system hardware and software, DMDC personnel decrease their ability to ensure emerging threats and identified vulnerabilities are adequately mitigated to preserve the overall security posture of DEERS. Furthermore, accurate inventories are necessary to effectively monitor, test, and evaluate security controls, and to support information technology planning,

¹⁴ Personnel used the Configuration Management Database to manage and track new, removed, or modified system hardware acquired in support of the DMDC mission.

budgeting, acquisition, and management. Because the Systems Division maintained enterprise-wide inventories of system hardware and software, those repositories could be adapted to maintain system-specific baselines, including one supporting DEERS, if Systems Division personnel revise the type of information currently required in each repository.

(FOUO) DMDC (b)(5) [Redacted]
[Redacted] In

In addition, we observed a storage room with multiple bins of degaussed hard drives that had been removed from service throughout an unknown number of years. The DMDC Seaside data center manager informed us that hard drives were not disposed because Systems Division personnel did not believe existing disposal procedures were sufficient to prevent residual data from compromise. The DMDC Seaside data center manager also stated that DMDC did not account for each hard drive once it was removed from service. Instead, he stated DMDC only accounted for the system hardware containing those hard drives within the DMDC (b)(5) [Redacted]. Because hard drives retain sensitive DEERS data until they have been degaussed, Systems Division personnel should adequately account for all hard drives removed from service to limit potential access to residual DEERS data.

According to the DMDC Problem Management team lead, DMDC personnel were in the process of developing procedures to record excess equipment in the DMDC (b)(5) [Redacted] and update the status of those assets in the Configuration Management Database. However, he could not identify when those procedures would be fully implemented. The lack of accountability over DEERS hard drives further illustrates the need for DMDC to maintain a configuration baseline of system-specific hardware from the point it's placed in service through such time personnel properly dispose of the system hardware or they provide the excess hardware to the Defense Reutilization Management Office.

(FOUO) DMDC (b)(5) [Redacted]
(FOUO) DMDC (b)(5) [Redacted]
[Redacted]

(FOUO) DMDC (b)(5) [Redacted]

(FOUO) DMDC (b)(5) [Redacted]

(FOUO) DMDC (b)(5) [Redacted]

Conclusion

Configuration management includes identifying and managing security features for all hardware, software, and firmware components of an information system, and systematically controlling changes to that configuration during the system’s lifecycle. Without testing all DEERS system hardware changes before implementing them in the production environment and documenting the impact changes could have on the overall DEERS security posture, DMDC personnel reduce their ability to effectively manage system changes and increases the risk that those changes will not operate as intended. Configuration management controls are critical to establishing an initial baseline of hardware, software, and firmware components and subsequently controlling and maintaining an accurate inventory of any changes to the system. However, DMDC personnel did not maintain a current and comprehensive baseline of DEERS system hardware and software, nor could they easily identify system-specific components in their Configuration Management Database.

(FOUO) DMDC (b)(5) [Redacted]

¹⁵ The Internet Assigned Number Authority is responsible for allocating and maintaining unique codes and a numbering system used in protocols supporting the Internet.

Management Comments on the Finding and Our Response

DMDC Comments

~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC agreed DEERS hardware changes were not always tested, DEERS system hardware and software was not easily identifiable, and ports and ^{DMDC (b)(5)} [REDACTED]

However, the Deputy Director partially agreed security assessments were not documented, stating IA impact assessments for DEERS application and operating system changes were evaluated when changes were assessed by the Development Steering Group. The Deputy Director acknowledged formal assessments were not completed, but IAO approval occurred as part of the Development Steering Group review and acceptance process.

Our Response

~~(FOUO)~~ Sound configuration management processes and procedures reduce risk and enable system owners to develop and maintain the integrity and security of information systems throughout their lifecycle. DMDC developed the DEERS Configuration Management Plan requiring key security-related decisions to be documented. However, DMDC acknowledged formal assessments evaluating the IA impact of proposed changes were not completed. We disagree the signature of personnel performing IA responsibilities constitutes a sufficient audit trail to support required security evaluations were properly completed. ^{DMDC (b)(5)} [REDACTED]

Recommendations, Management Comments, and Our Response

Revised and Renumbered Recommendations

As a result of management comments, we revised and renumbered draft Recommendation C.1.a as Recommendation C.1 and draft Recommendation C.1.b as Recommendation C.2 to further clarify the nature of actions needed to ensure all system security assessments were formally documented and system hardware changes were properly tested. We request that the Director, DMDC, provide comments on the final report by July 20, 2012. We also renumbered draft Recommendations C.2, C.3, C.4, and C.5 as Recommendation C.3, C.4, C.5, and C.6, respectively.

C. We recommend that the Director, Defense Manpower Data Center:

1. Revise the Defense Manpower Data Center Organizational Configuration Management Plan, Version 4.2, January 2009, the Defense Enrollment Eligibility Reporting System 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 Defense Manpower Data Center information systems, including the Defense Enrollment Eligibility Reporting System.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, disagreed, stating the DEERS IAO reviewed all functional specifications, which included a section to identify specific security issues, for projects reviewed by the Development Steering Group.

Our Response

The DMDC comments were nonresponsive to the intent of our recommendation. The Development Steering Group, which is comprised of DISSG personnel responsible for DMDC system security matters, may have evaluated DEERS application and system hardware changes; however, a documented audit trail supporting the decision making process was not kept. In responding to the finding, the Deputy Director stated DMDC did not maintain documentation, other than an IAO signature, supporting whether IA impact assessments occurred. The Information Technology Service Management Change Management Technical Review Board and CCB Process, November 9, 2010, states the DISSG is responsible for reviewing proposed configuration changes if they are submitted for review. However, the documentation also shows all changes may not necessarily be submitted for DISSG review depending on the priority of the change.

DMDC already developed tools that could provide a historical record of all analysis to support each proposed change had been properly assessed for IA impact, but has not required members of the Development Steering Group and the DISSG to use those systems to record their decisions. We believe those systems could easily support key risk management decisions affecting whether proposed changes impact the operational behavior of the device or potentially violate overall network and security policy. Therefore, we request the Director, DMDC, reconsider her position and require key decisions potentially affecting the DEERS security posture to be assessed and documented, and provide comments on the final report by July 20, 2012.

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.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, disagreed stating the DMDC Quality Assurance branch tested all application changes before being approved for the production environment. Additionally, the Deputy Director stated the System Division had a similar process for testing system hardware configuration and infrastructure changes.

Our Response

~~(FOUO)~~ The DMDC comments were nonresponsive to the intent of our recommendation. We agree DMDC tested and documented the results of testing DEERS system software (application) changes. However, we disagree DMDC had a similar process for testing DEERS system hardware changes. The Information Technology Service Management Change Management Technical Review Board and CCB Process did not require all system hardware configuration management changes to be tested and the system hardware CCB Chair stated changes were tested only when the Technical Review Board or the CCB recommended testing. DMDC used the ^{DMDC (b)(5)} [REDACTED] to track and manage system hardware changes throughout their lifecycle;

^{DMDC (b)(5)} [REDACTED]

~~(FOUO)~~ Based on our review of documentation previously provided by DMDC, we revised this recommendation to clarify our intent that DMDC needed to revise the Information Technology Service Management Change Management Technical Review Board and CCB Process, November 9, 2010, ^{DMDC (b)(5)} [REDACTED]

[REDACTED]. Therefore, we request the Director, DMDC, reconsider her position and revise the existing process to ^{DMDC (b)(5)} [REDACTED]

^{DMDC (b)(5)} [REDACTED]

[REDACTED], and provide comments on the final report by July 20, 2012.

3. Include the Defense Manpower Data Center information assurance manager or his written designee as an active and required member of the application and system hardware Configuration Control Boards.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, disagreed stating the CCBs were a virtual board that was part of an automated workflow process. The Deputy Director also stated the IAM or an approved delegate was part of the approval process for changes that go through the CCB review process.

Our Response

The DMDC comments were partially responsive to the intent of the recommendation. Documentation provided by DMDC did not specifically support the IAM or an approved

delegate had been appointed to the DEERS system hardware and software CCBs. The Information Technology Service Management Change Management Technical Review Board and CCB Process, which establishes and describes responsibilities of the system hardware CCB, identifies members of the system hardware CCB; the IAM or an approved delegate are not specifically included as members of the system hardware CCB team. In addition, the DEERS Configuration Management Plan, which establishes and describes responsibilities of the software application CCB, identifies groups included in the software application CCB. The software application CCB Chair and Quality Assurance manager informed us the IAM was not an appointed member of the software application CCB.

Regardless of whether the CCBs meet face-to-face or through an electronic medium, the IAM or an approved delegate is required to be a designated member of the CCBs to ensure security-related matters are fully addressed. Therefore, we request the Director, DMDC, reconsider her position and designate the IAM or an approved delegate as an official member of both the system hardware and software CCBs, and provide comments on the final report by July 20, 2012.

4. Update the existing Defense Manpower Data Center 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 Defense Enrollment Eligibility Reporting System-specific system hardware and software.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, partially agreed stating the Systems Division maintained a comprehensive list of system hardware and software. However, the Deputy Director also acknowledged the System Division did not specifically maintain a baseline showing which system the system hardware or software supported.

Our Response

The DMDC comments were nonresponsive to the intent of our recommendation. We agree DMDC maintained enterprise-wide repositories of system hardware and software. However, not only are system-specific baselines critical to effectively monitoring, testing, and evaluating security controls, they are required by DoD Instruction 8500.2 controls DCHW-1 and DCSW-1. During the October 2010 annual IA assessment, DMDC did not provide the independent contractors an accurate inventory of system hardware supporting DEERS operation. ^{DMDC (b)(5)}

We continue to believe DMDC could leverage its existing efforts to maintain enterprise-wide system hardware and software repositories by including fields that specifically identify which accreditation boundary (system) the asset supports. Therefore, we request the Director, DMDC reconsider her position and update existing system databases to require the accreditation boundary (system) using the system hardware and software, and provide comments on the final report by July 20, 2012.

5. Develop and implement procedures to account for system hardware throughout the complete lifecycle of that equipment, including hard drives, that process or store sensitive Defense Enrollment Eligibility Reporting System data.

DMDC Comments

The Deputy Director, DMDC, responding on behalf of the Director, DMDC, disagreed stating DMDC managed systems and components throughout their lifecycle by tracking, degaussing, and documenting failed or replaced hard drives.

Our Response

~~(FOUO)~~ The DMDC comments were partially responsive to the intent of our recommendation. Although we agree hard drives were degaussed and included a tag showing this, we disagree that DMDC personnel tracked and documented the status of all hard drives. The DMDC Seaside data center manager stated DMDC used the ~~DMDC (b)(5)~~ to track the lifecycle of the cabinets or racks holding the hard drives, but not the specific hard drives themselves. Additionally, he stated the tags on removed hard drives did not show which system the hard drives supported. Further, the DMDC Problem Management team lead confirmed disk drives were not tracked in the ~~DMDC (b)(5)~~ by serial number. During the audit, DMDC personnel did not provide documentation showing they tracked and accounted for individual disk drives from DEERS servers. Therefore, we request the Director, DMDC, reconsider her position and implement procedures to account for all DEERS hard drives throughout their lifecycle, and provide comments on the final report by July 20, 2012.

~~(FOUO)~~ 6. ~~DMDC (b)(5)~~

DMDC Comments

~~(FOUO)~~ The Deputy Director, DMDC, responding on behalf of the Director, DMDC, ~~DMDC (b)(5)~~

Our Response

~~(FOUO)~~ The DMDC comments were responsive; ~~DMDC (b)(5)~~

Appendix A. Scope and Methodology

We conducted this review from December 2010 through February 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform our work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on the objectives.

~~(FOUO)~~ We visited DoD Center Monterey Bay, the DEERS Project Management Office, in Seaside, California; the SMC in Auburn Hills, Michigan; and the Army Research Lab in Adelphi, Maryland. DEERS is a mission assurance category II system that processes sensitive data and, therefore, subject to 107 DoD Instruction 8500.2 IA controls. We reviewed whether DMDC and SMC Auburn Hills personnel adequately implemented 73 security design and configuration, identification and authentication, enclave and computing environment, enclave boundary defense, physical and environmental, personnel, and vulnerability and incident management controls.

We conducted walkthroughs of the DoD Center Monterey Bay and SMC Auburn Hills facilities, to include the data centers hosting the DEERS production, contingency failover, and test servers to evaluate physical and environmental controls. We interviewed the DMDC Seaside data center manager, facilities manager, and security specialists, as well as a SMC Auburn Hills technical consultant (contractor) to determine how both organizations managed access to the data centers and protected the DEERS operating system from environmental damage.

We also interviewed personnel from the DEERS and Systems Divisions and DISSG responsible for managing and implementing information security over the DMDC network and DEERS, including the CIO, IAM, DEERS IAO, information security specialists, database administrators, and SAs. In addition, we interviewed the DEERS Director, information technology and management specialists, SAs, the DMDC Seaside data center manager, change management team leads, developers, the DEERS chief architect, and the quality assurance manager to discuss the DEERS configuration management processes.

We developed non-statistical samples to further evaluate the effectiveness of DMDC processes to develop and maintain documentation that supported whether:

- ~~(b)(5)~~ DMDC (b)(5) SMC Auburn Hills and ~~(b)(5)~~ DMDC (b)(5) DMDC personnel took annual security awareness training;
- ~~(b)(5)~~ DMDC (b)(5) DEERS software application changes included an IA impact assessment, test plans and results, functional and technical requirements, and CCB approval;
- ~~(b)(5)~~ DMDC (b)(5) DEERS system hardware changes included an IA impact assessment, test results, and Technical Review Board and CCB approval;

- ^{DMDC (b)(5)} SMC Auburn Hills and ^{DMDC (b)(5)} DMDC personnel signed and acknowledged their understanding for accessing DMDC resources, including DEERS;
- ~~(FOUO)~~ SAs and database administrators with privileged access to ^{DMDC (b)(5)} ^{DMDC} DEERS contingency failover, test, and production servers had been granted access based on written authorization forms; and
- ~~(FOUO)~~ ^{DMDC (b)(5)} DEERS contingency failover, test, and production servers existed at DMDC Seaside.

We obtained and reviewed seven contracts, valued at approximately \$80.8 million in FY 2011 that DMDC had in place to obtain IA services and key management support for DMDC operations, including DEERS (see the table below).

~~(FOUO)~~ Table. DMDC Contracts for IA Services and Management Support

Contractor	Contract Number and Date of Contract	Scope of Contract	^{DMDC (b)(5)}
Deloitte and Touche	HHSN263999900031I, dated September 23, 2010	Program Management and Operational Support Services	
Telos	FA8771-04-D-0009, dated September 15, 2010	Information Technology Security Support	
Northrop Grumman	HHSN263999900041I, dated September 8, 2010	Information Technology Security Support	
Hewlett Packard ²	HC1028-08-D-2018, dated September 4, 2008	Host Production Support	
Hewlett Packard ²	GS-35F-0323J, dated February 27, 2008	System Development and Configuration Management Support	
Systems Research and Applications	GS-35F-4594G, dated February 14, 2008	Architectural Design, Software Development, and Database Management Services	
Hewlett Packard ²	W91QUZ-06-D-0013, dated September 24, 2007	Enterprise-wide Device Management and Network Services	

¹ ^{DMDC (b)(5)}

² This contract was initially awarded to Electronic Data Systems before being acquired by Hewlett Packard.

~~(FOUO)~~ In addition, we also obtained and reviewed the June 19, 2007, service level agreement between DMDC and the Army Research Lab to determine the scope of computer network defense services supporting DMDC network activities. Further, we obtained and reviewed the DMDC IA Policy, November 4, 2009; the DMDC Organizational and DEERS Configuration Management Plans, January 2009; various Unix and Oracle account access standard operating procedures, IA appointment letters, IA Vulnerability Alert notifications, DEERS interconnection memorandums of understanding, DMDC network and DEERS audit logs, and among other documentation, the October 2010 DEERS and DMDC enclave IA control test results to determine the effectiveness of DMDC's implementation of DEERS IA controls.

Use of Computer-Processed Data

We relied on computer-processed data from three separate DoD and commercial databases DMDC used to support its implementation of DoD Instruction 8500.2 controls DCSQ-1, DCCT-1, and PRTN-1. Specifically, we used data from the DMDC Change Management System and ^{DMDC (b)(5)} to evaluate the effectiveness of the DEERS system hardware and application software configuration management processes. In addition, we obtained information from the Booze Allen Hamilton Learning Management System to evaluate whether DMDC personnel completed annual security awareness training.

DMDC personnel used the Change Management System and ^{DMDC (b)(5)} as a repository to support the history of DEERS configuration management changes. We compared and validated the information obtained to support non-statistically selected samples from the Change Management System against other corroborating documentation, such as quality assurance test results and functional requirements. Because personnel did not maintain an audit trail supporting the decisions of the CCB, we relied on the information in these systems to evaluate whether DEERS system hardware and software changes were approved for production. In addition, we relied on information in the ^{DMDC (b)(5)} to determine whether DEERS system hardware changes had been tested because additional documentation was not available for review. However, none of the information we obtained from these systems was the result of database processing.

In addition, DMDC used the Learning Management System to account for personnel that completed annual security awareness training. After DMDC personnel completed training, their status was automatically updated in the system. DMDC personnel relied on the accuracy of this commercial system because they did not retain annual IA training completion certificates for their personnel; they only retained training certificates supporting the completion of initial training that resulted during the initial vetting process. Therefore, the information in the Learning Management System was the only source of data we could evaluate to determine whether personnel in our non-statistical sample had completed security awareness training. The information we relied on was not the result of any computer processing from this database.

Although we did not perform additional procedures to specifically test controls over the Change Management System, ^{DMDC (b)(5)} and Learning Management System, we did not find inaccuracies that would preclude the use of the computer-processed data to meet the objective of this audit or that would change the conclusions reached in this report.

Use of Technical Assistance

The Quantitative Methods and Analysis Division of the DoD Office of Inspector General provided assistance in developing our methodology for selecting non-statistical samples.

Prior Coverage

No prior coverage has been conducted on DEERS IA controls during the last 5 years.

(FOUO)

DMDC (b)(5)

(FOUO)

DMDC (b)(5)

(FOUO)

DMDC (b)(5)

Appendix C. Controls With Weaknesses Affecting the DEERS Security Posture

DMDC (b)(5)

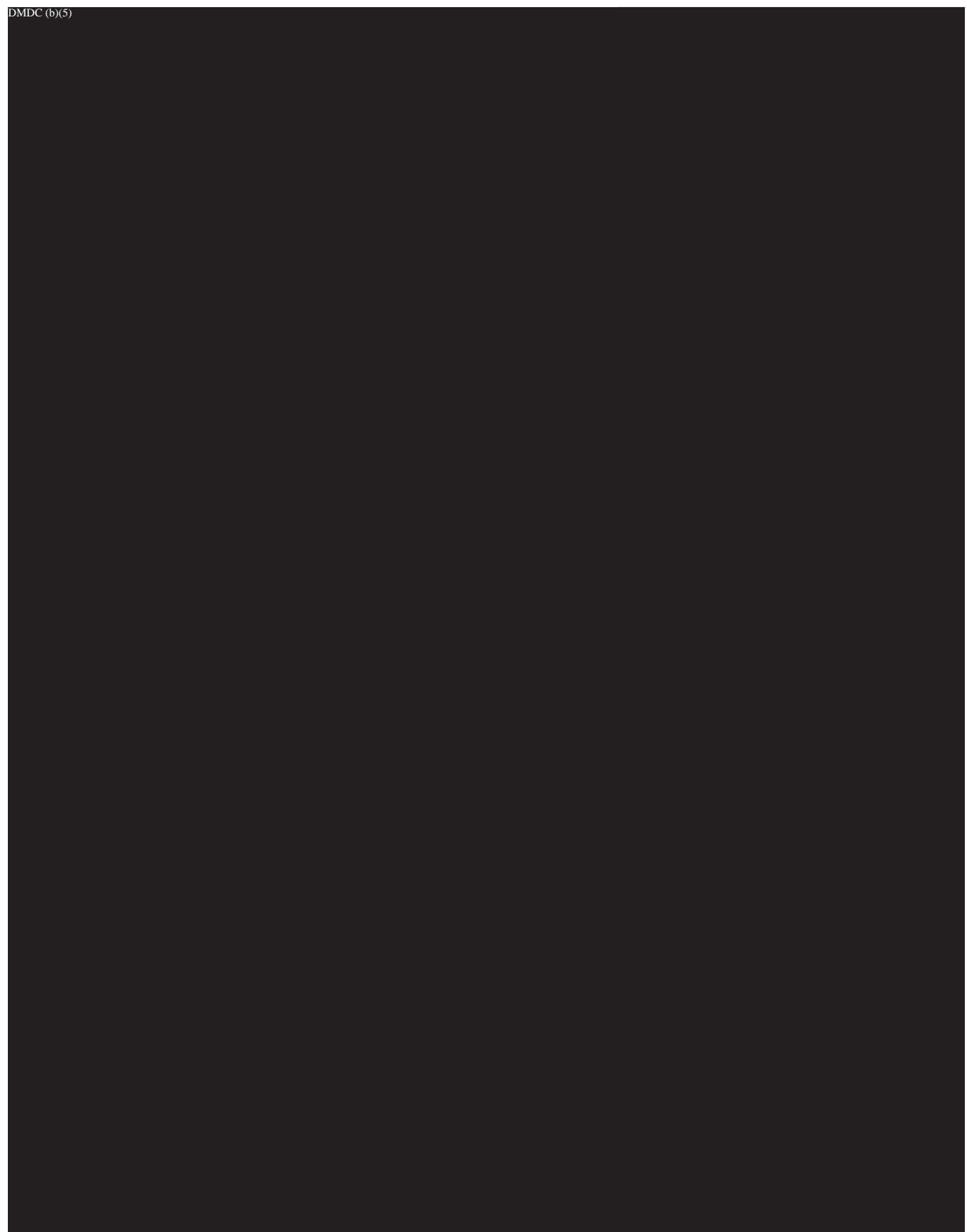
[Redacted]

Table. DMDC (b)(5)

DMDC (b)(5)

[Redacted Table Content]

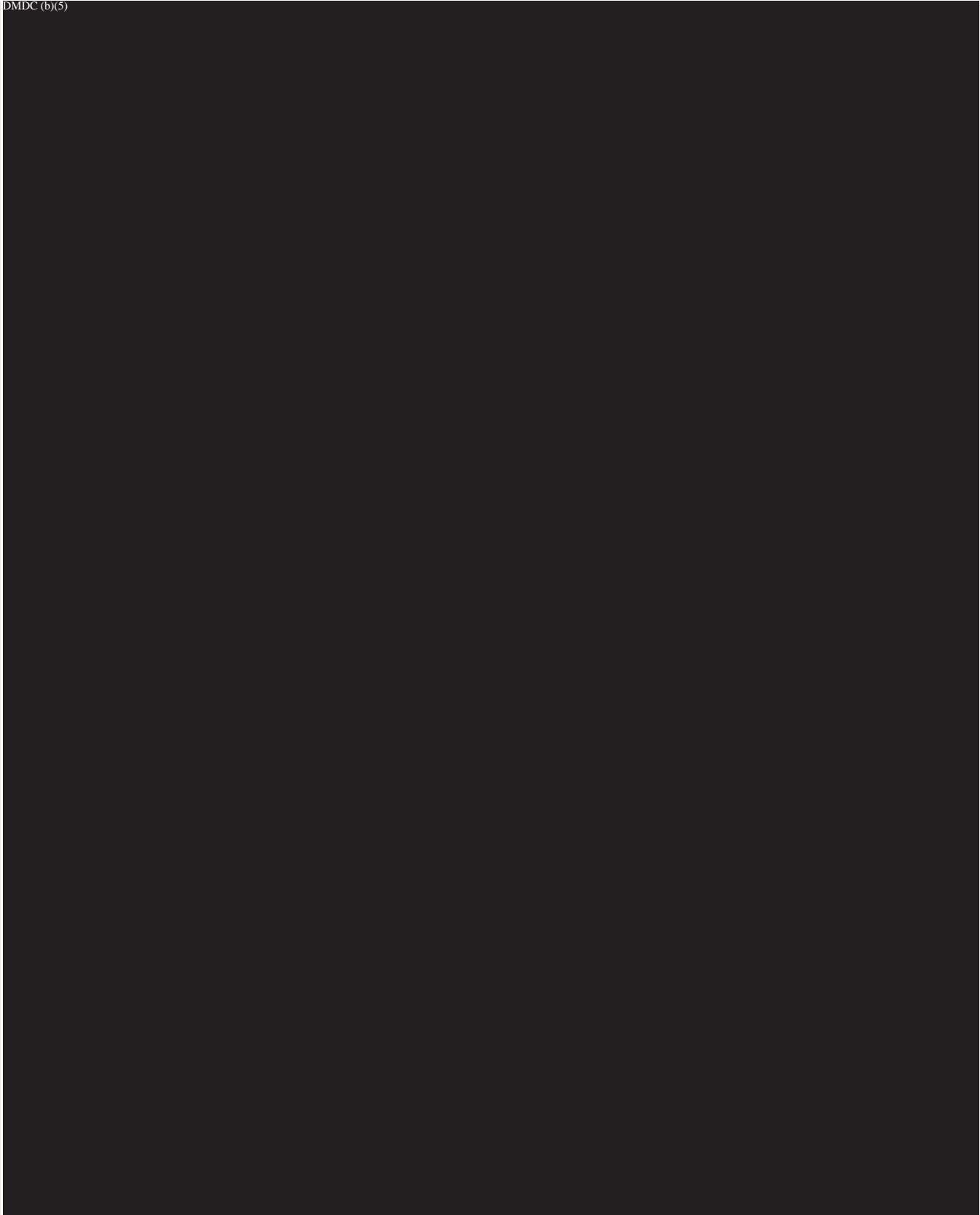













DMDC (b)(5)



Appendix D. Controls Without Significant Weaknesses

The table below identifies DMDC (b)(5) IA controls reviewed that DMDC personnel implemented without significant weaknesses. Implementation of those controls strengthened the overall DEERS security posture.

Table. Implemented Controls That Strengthened the DEERS Security Posture

	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
DMDC (b)(5) 			

	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
--	--	--------------------------	-----------------------------

DMDC (b)(5)



	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
--	--	--------------------------	-----------------------------

DMDC (b)(5)



	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
--	--	--------------------------	-----------------------------

DMDC (b)(5)



	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
--	--	--------------------------	-----------------------------

DMDC (b)(5)



	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
DMDC (b)(5)			

	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
--	--	--------------------------	-----------------------------

DMDC (b)(5)



	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
DMDC (b)(5)			

	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
DMDC (b)(5)			

	DoD Instruction 8500.2 Control Number	Subject Areas	Control Descriptions
DMDC (b)(5)			

Glossary

~~(FOUO)~~ **Audit Daemon.** A service or process that runs in the background during operations to record or capture detailed information about specific user actions, including the identification of altered data, types of system errors, and specific that has been accessed.

Audit Trail. A record of activity that is maintained to provide a basis for reconstructing or reviewing user activities.

Computer Network Defense. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.

Confidentiality Level. Establishes acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access an information system.

Configuration Management. Processes and procedures for monitoring the status of security controls and identifying potential security-related problems related to information systems.

Conformance Testing. A process for determining whether a system meets requirements or specific standards necessary for achieving connectivity or interoperability.

Data Integrity. Processes and procedures designed to ensure data are protected against unauthorized modification or destruction that could reduce a user's reliance on the data.

Database. A collection of related information about a subject that is organized in a useful manner to provide a basis for procedures, such as retrieving information, drawing conclusions, or making decisions.

Database Administrator. An individual responsible for designing a database, to include its structure and content, and administering access to users of the database.

Degauss. A procedure that renders previously stored data on magnetic media unreadable by applying a reverse magnetizing field.

Enclave. A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy.

Firewall. Hardware and software components that permit authorized users to access and transmit information, as well as deny access to unauthorized users.

Information Assurance. The measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance Manager. An appointed official responsible for implementing an IA program for an information system or organization within DoD.

Information Assurance Officer. An appointed official responsible for maintaining an appropriate operational IA posture of an information system or organization within DoD.

Information Assurance Vulnerability Alert. A comprehensive process that notifies DoD personnel about vulnerabilities affecting their information systems and networks; they include implementation strategies to reduce the risk associated with identified vulnerabilities.

Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Information Technology. Any equipment or interconnected system or subsystem used in the automatic acquisition, storage, manipulation, management, movement, control, display, interchange, transmission or reception of data or information.

Interconnection. A direct connection between two or more information systems established for sharing data and other information resources.

Intrusion Detection System. A device that inspects activity occurring within a network or specific host to identify suspicious patterns that may indicate an attack from someone attempting compromise a system or network.

Least Privilege. Access privileges that allow a user to only perform functions or access information required to complete assigned duties.

Logical Access. Technical controls within an information system that limit and control access to data or the information system.

Mission Assurance Category. The classification assigned to DoD information systems, which reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the war fighters combat mission, and are primarily used to determine the requirements for availability and integrity.

Need-to-Know. The necessity for access to, or knowledge of, specific DoD information required to carry out official duties.

Network. A group of computers and associated devices that are connected by communication lines, routers, hubs, and technical control devices.

Operating System. The software that controls the execution of other computer programs, schedules tasks, allocates storage, manages the interface to peripheral hardware, and presents a default interface to the user when no application program is running.

Penetration Testing. A testing methodology in which assessors attempt to circumvent or defeat the security features of an information system.

Port. The logical connection point that enables the transmission of information from computer to computer.

Privileged Access. An authorized user who has access to system control, monitoring, or administration functions that an ordinary user would not have.

Protocol. A standard that specifies the format of data, as well as the rules to be followed when performing specific functions.

Public Domain Software. Software, also known as open-source code, which has been distributed for unconditional use without warranty.

Quality Assurance. Processes and procedures that are implemented to ensure functional and technical requirements are met.

Remote Access. The process of communicating with a computer located in another place over a communications link.

Risk Management. The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

Sensitive Information. Any data in which the loss, misuse, or unauthorized access to, or modification of, could adversely affect our national interests or DoD mission.

Service Level Agreement. The agreed framework for the delivery of services and the measurement of service quality that is negotiated between the provider and the user to ensure that the expectations of service are realistic and within the provider's capabilities.

System Administrator. An individual that is responsible for administering the use of multiuser computer or communications systems.

Threat. A circumstance or event that could adversely impact organizational operations and assets, individuals, other organizations, or the Nation, through an information system by unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerability. The weaknesses in an information system, system security procedures, or internal controls that could be exploited or triggered by the source of a threat.

Defense Manpower Data Center Comments




DEPARTMENT OF DEFENSE
DEFENSE HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
4800 MARK CENTER DRIVE, SUITE 04E25-01
ALEXANDRIA, VA 22350-4000

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DMDC Response to OIG Draft Final Report (FOUO), "Improvements Needed to Strengthen the DEERS Security Posture," (Project Number D2011-D000FG-0088)

Thank you for the opportunity to review and provide comments on the draft report, "Improvements Needed to Strengthen the DEERS Security Posture," Project No. D2011-D00FG-008.

The Defense Manpower Data Center's response to the draft report recommendations is included in the attachment. My point of contact for this matter is [REDACTED]. She is reachable at [REDACTED].

for 
BRECKENRIDGE, MARK.
STEPHEN [REDACTED]
Mary Snavelly-Dixon
Director

Attachment:
As stated

DMDC Comments to DoD OIG Report Improvements Needed to Strengthen the DEERS Security Posture

INTRODUCTION

DMDC has reviewed the DRAFT DoD OIG Report referenced above and provides the following comments. We have divided our comments into sections that correspond to the OIG report division of Findings, and Recommendations.

FINDINGS

FINDING A. Improvements Needed To Strengthen the DEERS Security Posture

A.1. Security Measures Were Insufficient to Identify and Protect the Defense Enrollment Eligibility Reporting System from Known Vulnerabilities

DMDC Position: Partially concur.

DMDC (b)(5)

(1) We perform exhaustive vulnerability testing annually as part of FISMA security certification testing and create a formal POA&M based on the results. In addition, DMDC scans all assets monthly using Retina to confirm the progress and effectiveness of the ongoing mitigation and patching efforts related to the POA&M. Furthermore, as patches are applied, we execute specific targeted vulnerability scans to confirm the patching.

(2) Oracle releases quarterly security patches for Solaris and for Oracle database software. With the release of quarterly patches, we validate and test the patches for the DEERS operating environment and then schedule the application of the patch during the next maintenance window, typically no less DMDC (b)(5) after completion of validation testing of the patch. Because of the quarterly release and patch cycle, IAVAs related to Oracle products frequently go under POA&M. Since DEERS relies heavily on Oracle products, this gave the appearance to the audit team that patches lagged.

(3) McAfee UVSCAN anti-virus used on our UNIX servers does not support automated updates; however, DMDC is DMDC (b)(5), we have instituted processes to update the signatures manually and regularly.

Although we can always strengthen security measures, we do not concur with the sentiment conveyed by the statement that protection of DEERS is not sufficient. DMDC (b)(5)

We are also evaluating specific STIG compliance tools such as Tripwire's Configuration Assessor.

A.2. Risk Management Processes and Procedures Needed Improvement

~~FOR OFFICIAL USE ONLY~~

DMDC Position: Concur.

A.3. DEERS Audit Log Data Was Not Reviewed or Secured

DMDC Position: Partially concur.

This assertion is overly broad and not supported by the facts. Although we can make improvements, DEERS-related audit data is both reviewed and secured. The audit team correctly observed that no regularly scheduled, formal review occurs and that audit logs are typically reviewed in response to events rather than pro-actively. DMDC secures audit data by ACLs and only administrators have access to them. The primary objection was the protection of audit data from system administrators with root privileges. ~~DMDC (b)(5)~~

However, to assert that this makes the Audit Log Data unsecured is an exaggeration.

A.4. Additional Safeguards Needed to Protect DMDC Network Devices and the DEERS Operating System

DMDC Position: Partially concur.

The OIG assertions include: (1) absence of control of logical access to network security devices; (2) VPN communications within the DMDC enclave were not visible to a network IDS; and (3) lack of configuration of host-based IDS on DEERS servers.

(1) The handling of strict control and management of logical access to network security devices, including firewalls, VPNs, proxies, and IDS devices is accomplished by the Network branch of the Systems Division.

(2) IDS decrypts and monitors our external VPNs at the network perimeter. Although not required, some internal communications are conducted within a VPN rather than using unencrypted network transmission. These internal communications are not visible to an IDS.

(3) Host-based IDS (Tripwire) was not configured on 13 of 62 DEERS-related servers. DMDC has addressed this (see Recommendation A.9 below).

FINDING B. Stronger Controls Needed to Prevent Unauthorized Access

B.1. Improvements Needed to Account for Personnel Supporting DEERS

DMDC Position: Partially concur.

The OIG cites three findings to support this conclusion: (1) absence of appointments in writing of SAs and DBAs; (2) out-processing control is inadequate; and (3) eight out of 203 DEERS-related contractor email accounts accepted email addresses without the CTR designation.

(1) DEERS is only one of many major systems operated by DMDC. The STS Division provides system administration services for all of the systems, including DEERS, and does not necessarily distinguish accreditation boundaries. We fully vet all system administrators at an appropriate level and maintain the required DoD 8570.01 IA certifications. STS provides Enterprise DBA services in a similar manner; however, specific projects may provide application DBAs, with lesser privileges. The OIG correctly observed that the appointment of SAs and DBAs are not explicitly in writing to specific projects.

Revised

(2) DMDC policy requires that all out-processed employees have all system privileges revoked as well as their CAC. The DEERS IAO maintains a list of all DEERS employees and ensures the removal of privileges and accounts for departing employees. The OIG's assertion was largely based on the existence of a tickler Checklist for out-processing in the DMDC IA Policy. The OIG asked to see completed checklists for departed employees. Checklists are not required to be retained and were not available for review. As an alternative, we suggest the effectiveness of DMDC's revocation process can be effectively determined by conducting an audit of personnel who have departed to see if DMDC revoked physical and logical access privileges. The DMDC Security Officer selected 15 departed personnel at random, and researched to determine if revocation of access privileges occurred. In all cases, we found effective and correct revocation of physical and logical access permissions for the departed. DMDC will document audits of access revocation for departed personnel as a means of confirming adherence to policy.

(3) DMDC policy requires that all contractor email addresses end in .ctr. This policy is in place and enforced. The eight accounts cited had the correct email address but they also had an overlooked alternative alias that we since corrected.

B.2. Access to DEERS and DMDC Network Devices Was Not Effectively Managed

DMDC Position: Non-Concur.

The Network branch of the STS Division strictly controls all access to network devices. Only a very small number of administrators have access to these devices. Furthermore, the use of Tripwire for Enterprise to verify the configuration of all network devices occurs every 15 minutes.

B.3. Additional Protection Needed for DMDC Seaside Data Center

DMDC Position: Concur.

See Recommendation B.1.I for description of additional safeguards that DMDC is implementing.

FINDING C. Weakness Existed in DEERS System Configuration Management Process

C.1. Security Assessments Were Not Documented

DMDC Position: Partially concur.

We perform Security assessments annually as part of FISMA security testing and are documented as a Risk Assessment provided with an Executive DIACAP package. The IA impact for application and system level changes is evaluated for changes that go before the DSG; however, a formal assessment is not prepared other than the IAO sign-off for specific security evaluation that is part of the DSG review and acceptance process.

C.2 DMDC (b)(5)

DMDC (b)(5)

C.3 DMDC (b)(5)

DMDC (b)(5)

Revised

~~DMDC (b)(5)~~
~~DMDC (b)(5)~~

RECOMMENDATIONS

RECOMMENDATION A.

A.1. Update the Defense Manpower Data Center Information Assurance Policy, November 4, 2009, to require:

- (a) Systems and Technical Support Division personnel 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.
- (b) Systems and Technical Support Division personnel formally document and submit the results of periodic vulnerability assessments to the Defense Manpower Data Center Information Systems Security Group to ensure it properly manages known vulnerabilities affecting the agency's information systems.
- (c) System owners prepare formal risk assessments that are approved by the Defense Manpower Data Center chief information officer before outsourcing key information assurance services.
- (d) Technology Steering Group personnel formally document evaluations that support the risk of using public domain software on Defense Manpower Data Center information systems and that are approved by the Defense Manpower Data Center Designated Accrediting Authority.

DMDC Response: Concur.

DMDC will update the IA Policy to include the OIG recommendations. Current IA Policy contains general language requiring compliance to all Federal and DoD requirements. We will add specific guidance to address the areas of vulnerability assessments and review, risk assessments, and the use of both public domain and open source software.

Although the recommendation is for policy changes, it incorrectly implies that DMDC does not perform monthly vulnerability scans, and that when it does perform scans, the results are not reviewed. Our monthly scans typically duplicate the results of already known vulnerabilities being worked in an existing POA&M. Monthly scans, along with ad-hoc targeted scans are used to verify results for specific patches and remediations.

A.2. Perform penetration testing of the Defense Enrollment Eligibility Reporting System to verify Defense Manpower Data Center management actions are sufficient for mitigating the risk of cyber attacks against the system.

DMDC Response: Concur.

The IA Branch will prepare plans for targeted penetration testing of DEERS and will engage internal security experts, external groups, or both to perform penetration testing to the extent that budget resources are available.

Note: According to NSA Security Assessment of the top 20 Critical Controls (SANS poster, Winter 2012), penetration testing was identified as the least effective of critical security controls, number 20 out of 20, with Low attack mitigation and a technology with Low-Medium maturity. Hence, it competes for limited budget resources with other more effective security controls.

A.3. Complete ongoing evaluations to acquire up-to-date virus protection software that enables automated updates when the vendor deploys new virus protection capabilities and install the new software on all Defense Enrollment Eligibility Reporting System servers.

DMDC Response: Concur.

DMDC has deployed McAfee UVSCAN to all DEERS servers and has updated the virus protection signatures on all DEERS servers. UVSCAN does not support automatic update; however, DMDC is developing a script to schedule updates. In the meantime, we have instituted processes to update the signatures manually and regularly.

A.4. Encrypt sensitive Defense Enrollment Eligibility Reporting System data at rest in accordance with Defense Manpower Data Center Information Assurance Policy, November 4, 2009, requirements.

DMDC Response: Concur.

DMDC policy is that encryption of data at rest on servers and in databases is not necessary unless required by the information owner (this position is also consistent with DoDI 8500.2 IA control ECCR-1 as noted in the OIG report). The DMDC IA policy contained a clerical error in the table of requirements indicating that encryption for this data was required. We have corrected the IA Policy. The DEERS information owner currently does not require encryption of data-at-rest, relying instead on system mechanisms to secure the data. DMDC controls access by system permissions, ACLs, and application-specific authorization lists.

A.5. DMDC (b)(5)

DMDC (b)(5)

DMDC (b)(5)

A.6. Implement additional safeguards and procedures to protect the integrity of Defense Enrollment Eligibility Reporting System Unix operating system audit logs from system administrator actions that could bypass or negate existing security controls over the system.

DMDC Response: Partially concur.

DMDC has not limited the privileges of the root account on DEERS systems. It is frequently necessary that system administrators perform the role of auditor and have access to audit log information.

A.7. Configure all Defense Enrollment Eligibility Reporting System servers with fully functional auditing capabilities that allow all auditable data necessary to reconstruct the events of a security incident to be recorded.

DMDC Response: Concur.

All necessary and critical events and access should be logged. In some cases, logging all actions is not feasible.

A.8. Develop policy and procedures for managing, configuring, and securing Defense Manpower Data Center network devices.

DMDC Response: Partially concur.

The Network branch of the STS Division controls strictly all access to network devices. Only a small number of administrators have access to these devices. Furthermore, DMDC uses Tripwire for Enterprise to verify the configuration of all network devices every 15 minutes.

DMDC uses the CA Ticketing system to review, approve, and document all configuration changes.

Written SOPs exist for many processes but not all.

A.9. Deploy host-based intrusion detection systems on the 13 Defense Enrollment Eligibility Reporting System production, contingency failover, and test servers not currently protected by these security devices.

DMDC Response: Concur.

We use Tripwire to provide host-based intrusion detection on the DEERS servers. DMDC has installed agents on all 13 servers. We are actively monitoring DMDC the remaining two are pending network communication establishments to allow for continuous monitoring.

A.10. Review the performance of the officials responsible for managing the Defense Manpower Data Center information assurance program, including the Defense Enrollment Eligibility Reporting System security posture, and based on the results consider corrective actions, as appropriate to meet DoD Instruction 5500.2, "Information Assurance (IA) Implementation," February 5, 2003, information assurance requirements.

DMDC Response: Concur.

DMDC is revising the IA architecture to allow for greater surveillance and security oversight of operations and separation of duties. We have appointed a new CIO and IAM.

RECOMMENDATION B.

B.1.a. Develop a process to accurately account for, and periodically review, at least annually, Defense Manpower Data Center and Service Management Center Auburn Hills personnel with access to the Defense Enrollment Eligibility Reporting System operating system.

DMDC Response: Partially concur.

Processes exist for granting and managing access to the DMDC data center. The AH data center has strict access procedures in place; DMDC (b)(5)

B.1.b. Develop written procedures for granting access to the Defense Enrollment Eligibility Reporting System applications that enables the Division Director to hold application managers and site security managers accountable for managing and controlling access, to include maintaining required documentation that supports whether access to those applications had been properly authorized.

DMDC Response: Partially concur.

Revised

Revised

DMDC developed and published account management instructions for SSMs in the *Application Security Guide seven years ago*. Section 4.0 of this guide specifically requires that the SSM review the list of users at the site at least monthly and remove a user's access when the user: (1) no longer has a need for the application; (2) has been suspended from using the application; or (3) is no longer a user at that site. The User Manual for the Security Online Web Application describes how to remove a user's application access.

DMDC only maintains DD2875s for provisioning of the SSMs. SSMs are responsible for managing user access per written documentation.

DMDC does not perform regular audits of these SSM DD2875s. DMDC will evaluate the appropriate periodic audit requirements and intervals.

B.1.c. Review configuration settings to validate whether the automated functionality for deactivating accounts inactive for more than 60 days was properly configured and update automated system settings designed to control access to Defense Enrollment Eligibility Reporting System applications are fully functional to ensure inactive accounts are promptly deactivated.

DMDC Response: Concur.

Automated processes are in place to suspend accounts that are inactive for more than 120 days, rather than the stated requirement of 60 days. DMDC will revise these procedures to enforce a 60-day period.

One area of potential confusion during the OIG visit was the status of application accounts and the practice of suspending dormant accounts before final deactivation. Suspension is a form of deactivation; suspended accounts cannot be used for DEERS access without administrator intervention. Suspension of dormant accounts is the first step towards permanent deactivation. The primary difference is that the SSM can reinstate a suspended account, but with an account deactivation, a new account must be requested to regain access. An account that remains in a suspended state for another 120 days is deactivated. We do not believe the distinction between suspended and deactivated accounts was clear to the OIG audit team and they incorrectly left with the impression that suspended accounts could be used for DEERS access because they continued to show as "live" accounts, even though "suspended".

B.1.d. Appoint, in writing, system administrators, database administrators, and other Defense Manpower Data Center personnel performing information assurance roles and responsibilities in accordance with requirements in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD 8570.01-M, "Information Assurance Workforce Improvement Program," April 20, 2010.

DMDC Response: Partially concur.

For some applications and databases, these processes already exist. However, DMDC will institute procedures to appoint SAs and DBAs in writing for all systems. Note, however, DMDC appoints some system administrators at the enterprise level, rather than the project level. For example, a person may be appointed as a Solaris system administrator rather than explicitly named to be a Solaris system administrator for DEERS servers.

B.1.e. Comply with existing out processing procedures and documentation requirements defined in the Defense Manpower Data Center Information Assurance Policy, November 4, 2009, and establish a centralized function to validate whether required actions have been properly taken.

DMDC Response: Non-concur.
Refer to Finding B.1 (2) above for explanation.

B.1.f. Define a reasonable period of time to promptly deactivate and remove account access, and hold trusted agents accountable for completing those actions within that period.

DMDC Response: Non-concur.

See response to B.1.c. After a reasonable period, DMDC terminates access by suspending an account for use. This gives us the opportunity to reinstate infrequent, but authorized users, without the administrative overhead of new account initiation. Suspension does in fact terminate access and is logically equivalent to deactivation.

DMDC will develop processes for periodic review of active accounts.

B.1.g. Review existing contractor e-mail accounts to verify whether they have been properly configured to include a "ctr" affiliation display.

DMDC Response: Partially concur.

DMDC complies with DoD policy for contractor e-mail affiliation display. The eight cited examples were errors that we have corrected. DMDC will institute a process for periodic review of all contractor email accounts.

B.1.h. Reconcile and periodically, at least annually, revalidate whether personnel ~~DMDC (b)(5)~~ and require them to complete a Defense Manpower Data Center User Agreement.

DMDC Response: Partially concur.

DMDC will evaluate the feasibility of annual review of personnel access lists. The DMDC data center also hosts several tenant organizations.

DMDC will evaluate adding renewal of the required User Agreement as part of our annual Security Awareness training.

B.1.i. Review and periodically, at least annually, revalidate existing accounts for Defense Manpower Data Center and Service Management Center Auburn Hills personnel with physical and logical access to Defense Enrollment Eligibility Reporting System servers and databases, and reconcile those accounts to verify whether access was granted based on approved user access request forms.

DMDC Response: Partially concur.

Physical access is limited and controlled as all servers reside in a controlled access data center. DMDC will develop procedures to review logical access.

Revised

B.1.j. Revise and update existing procedures for granting access to Defense Manpower Data Center systems and resources, to include remote access, that address requirements for: (1) periodically revalidating the continued need for access; (2) supervisory review and documented approval of access; and (3) justifying the need and level of access requested.

DMDC Response: Partially concur.

Procedures are in place for justifying and granting remote access. DMDC will develop processes for periodic review.

B.1.k. Develop new or update existing data sharing agreements to verify whether agreements are in place that describes security requirements and the terms and conditions for transferring data between organizations authorized to receive Defense Enrollment Eligibility Reporting System data.

DMDC Response: Partially concur.

DMDC has data sharing agreements in place that include security requirements. DMDC is currently reviewing the terms of agreements and developing new agreements.

a.i.i. DMDC (b)(5)

DMDC (b)(5)

B.2. We recommend the Director, Defense Manpower Data Center, 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.

DMDC Response: Concur.

RECOMMENDATION C.

C.1. Revise the Defense Manpower Data Center Organizational Configuration Management Plan, Version 4.2, January 2009, and the Defense Enrollment Eligibility Reporting System Configuration Management Plan, Version 4.2, January 2009, to require that the:
(a) Development Steering Group formally evaluate and document the results of whether proposed configuration changes affect the overall security posture of Defense Manpower Data Center information systems, including the Defense Enrollment Eligibility Reporting System.
(b) Systems and Technical Support Division personnel test and document the results of testing all configuration changes that are approved to be implemented in the production environment.

DMDC Response: Non-concur.

The DEEERS IAO reviews all charters and functional specifications for projects that go before the DSG for security issues. The functional specification includes a required section that contains indicators of IAO review and IAO approval along with a table of specific security issues.

Revised and
Renumbered as
Recommendations
C.1 and C.2,
respectively

The Enterprise Service QA group tests all applications before deployment into production. STS Division has a similar process for testing and deploying configuration and infrastructure changes.

C.2. Include the Defense Manpower Data Center information assurance manager or his written designee as an active and required member of the application and system hardware Configuration Control Boards.

DMDC Response: Non-concur.

The Configuration Control Board is a virtual board, part of an automated workflow process. The IAM or delegate (IAO) is part of the approval process for items going through the CCB review process.

3. Update the existing Defense Manpower Data Center 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 Defense Enrollment Eligibility Reporting System-specific system hardware and software.

DMDC Response: Partially concur.

The STS Division maintains comprehensive, automated inventory of IT assets, including hardware, components, and software. STS does not track to which accreditation boundary, i.e. which system such as DEERS, particular assets belong. STS manages the server as a Solaris or Oracle server, not necessarily as a DEERS server.

4. Develop and implement procedures to account for system hardware throughout the complete lifecycle of that equipment, including hard drives, that process or store sensitive Defense Enrollment Eligibility Reporting System data.

DMDC Response: Non-concur.

Systems and components are managed throughout the lifecycle. We track, degauss, and document, per DoD and DMDC policy, failed or replaced hard drives.

5. DMDC (b)(5) [Redacted]

DMDC (b)(5) [Redacted]

[Redacted]

Renumbered as
Recommendation
C.3

Renumbered as
Recommendation
C.4

Renumbered as
Recommendation
C.5

Renumbered as
Recommendation
C.6

~~FOR OFFICIAL USE ONLY~~



Inspector General
Department of Defense

~~FOR OFFICIAL USE ONLY~~