Report No. DODIG-2016-123

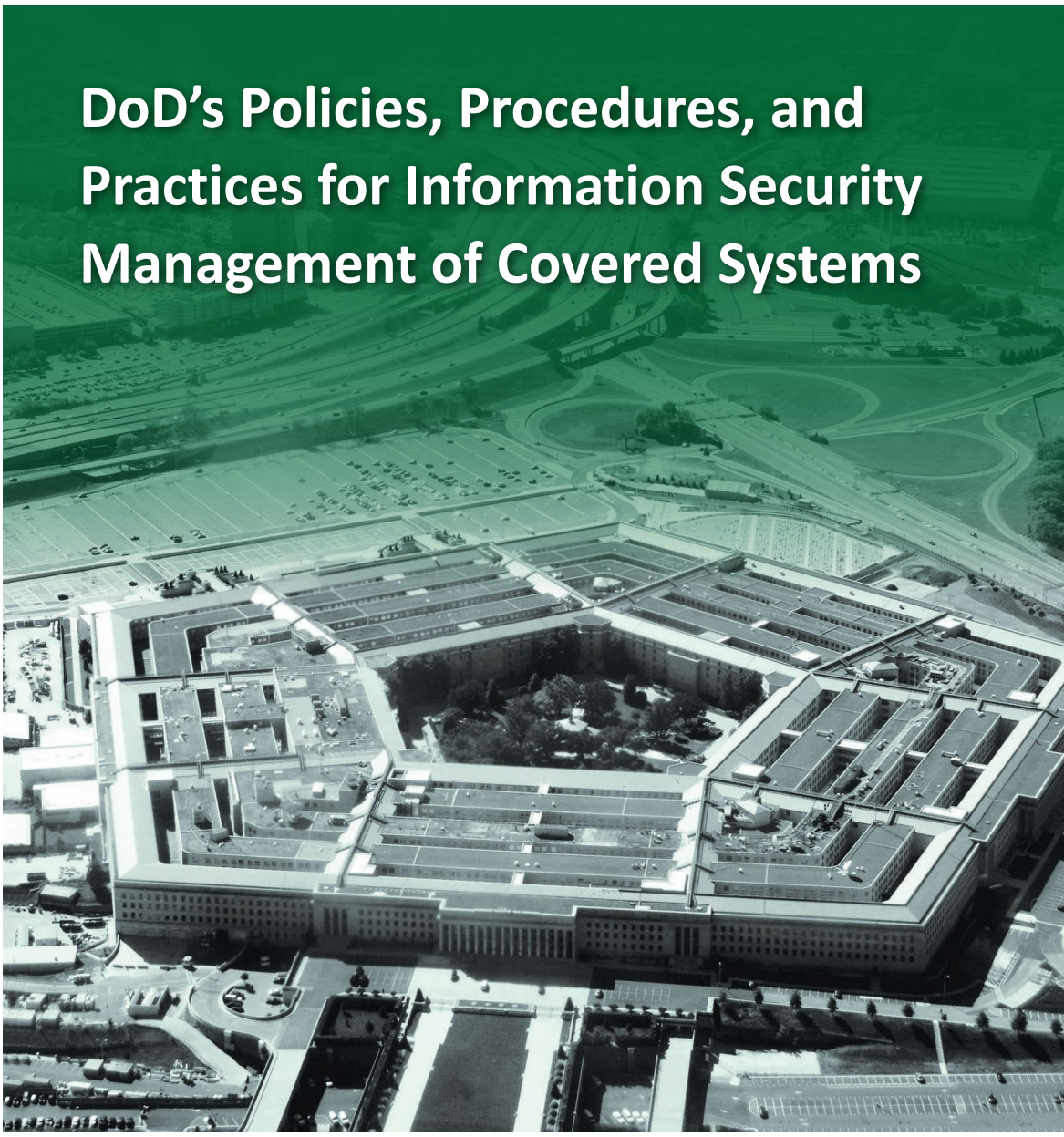
~~FOR OFFICIAL USE ONLY~~

# INSPECTOR GENERAL

*U.S. Department of Defense*

AUGUST 15, 2016

# DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

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

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

## Mission

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

## Vision

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


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

# Results in Brief

## *DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems*

**August 15, 2016**

## Objective

We summarized DoD's policies, procedures, and practices related to implementing logical access controls, conducting software inventories, implementing information security management, and monitoring and detecting data exfiltration and other cyber threats. We also assessed whether DoD Components followed logical access control policies, procedures, and practices. The DoD Office of Inspector General prepared this report in response to the requirements of the Cybersecurity Act of 2015, section 406, December 18, 2015.

## Results

The DoD has policies, procedures, and practices related to logical access controls, including multifactor authentication;[1] software and license inventories; monitoring and threat detection capabilities; and information security requirements for third-party service providers. In summary:

- The DoD issued logical access policies, including policies requiring the use of multifactor authentication. In addition, DoD network and system owners issued procedures for implementing logical access controls using the National Institute of Standards and Technology catalog of system and privacy controls. However, the DoD audit community identified instances of DoD Components not following logical access control requirements.
- The DoD issued policies that require system owners to conduct inventories of software. However, the DoD did not have policy for conducting software license inventories. Officials with the DoD Office of the Chief Information Officer stated that they are establishing an agencywide policy for conducting software license inventories in response to a 2014 recommendation in a Government Accountability Office report. Although the DoD did not have an agencywide policy, three DoD Components had policies for conducting inventories for software licenses.
- The DoD Components reported using capabilities to monitor networks and systems to detect threats and data exfiltration. Those capabilities include the use of firewalls, host-based security systems, intrusion detection systems, intrusion prevention systems, and network analysis tools.
- The DoD issued policies that require DoD Components to ensure third-party service providers implement information security management practices such as conducting software inventories and deploying threat monitoring and detection capabilities.

## Recommendations

In this report, we identify recommendations from previous audits. Therefore, this report contains no new recommendations and is provided for information purposes only.

## Management Comments

Because the report does not contain new recommendations, we did not request management comments.

[1] Authentication is the process of verifying the identity of a user or verifying the source and integrity of data. The Act defines multifactor authentication as the use of not fewer than two authentication factors, such as:

- something known to the user, such as a password or personal identification number;
- an access device provided to the user, such as a cryptographic identification device or token; or
- a unique biometric characteristic of the user, such as fingerprints or face recognition.

*Visit us at www.dodig.mil*


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

August 15, 2016

MEMORANDUM FOR DISTRIBUTION

SUBJECT: DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems (Report No. DODIG-2016-123)

We are providing this report for your information and use. We prepared this report to satisfy the requirements of the Cybersecurity Act of 2015. The report shows that the DoD has policies, procedures, and practices related to logical access controls, including multifactor authentication; software and license inventories; monitoring and threat detection capabilities; and information security requirements for third-party service providers. Although this project was announced as an assessment, we did not conduct an audit, assessment, or evaluation in accordance with applicable standards. We did, however, perform this effort in accordance with applicable standards of the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Federal Offices of Inspector General," August 2012.

In this report, we identified recommendations from previous audits. Therefore, this report contains no new recommendations and is provided for information purposes only. Because the report does not contain new recommendations, we did not request management comments.

We appreciate the courtesies extended to the staff from the DoD Chief Information Officer and the nine DoD Components that provided data. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

***Distribution:***

COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE HUMAN RESOURCES ACTIVITY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, DEFENSE HEALTH AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
NAVAL INSPECTOR GENERAL

# Contents


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

# Introduction

## Objective

Our objective was to describe the DoD's policies, procedures, and practices for implementing logical access controls, conducting software inventories, implementing information security management, and monitoring and detecting data exfiltration and other cyber threats. We also assessed whether DoD Components followed the logical access control policies, procedures, and practices. Although this project was announced as an assessment, we did not conduct an audit, assessment, or evaluation in accordance with applicable standards. We did, however, perform this effort in accordance with applicable standards of the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Federal Offices of Inspector General," August 2012.

## Background

The DoD Office of Inspector General prepared this report in response to the requirements of the Cybersecurity Act of 2015, section 406, December 18, 2015. See Appendix A for a discussion of the scope and methodology. Ten DoD Components provided input for this report: the DoD Chief Information Officer, Department of the Army, U.S. Marine Corps, Department of the Navy, U.S. Air Force, Defense Information Systems Agency (DISA), Defense Finance and Accounting Service (DFAS), Defense Human Resources Activity, Defense Health Agency (DHA), and Missile Defense Agency (MDA). Each Component provided either Component- or system-level policies and procedures related to information security management.

Information security management includes practices designed to protect networks, systems, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. These practices include, but are not limited to, implementing appropriate logical access controls, conducting inventories of software and associated licenses, monitoring and detecting network and system threats, and ensuring third-party providers implement similar information security controls.

## Requirements of the Cybersecurity Act of 2015

The Cybersecurity Act (the Act) was enacted on December 18, 2015, and includes a requirement for Federal Inspectors General to generate a report describing agency policies, procedures, and practices for covered systems. The Act describes covered systems as national security systems[2] and Federal computer systems that provide access to personally identifiable information. The Act requires Federal Inspectors General to submit a report to the agency committees of jurisdiction in the Senate and House of Representatives within 240 days of enactment of the Act (August 14, 2016). The Act requires the report to include the following:

A. A description of the logical access[3] policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

B. A description and list of the logical access controls and multifactor authentication[4] used by the covered agency[5] to govern access to covered systems by privileged users.[6]

C. If the covered agency does not use logical access controls or multifactor authentication to access a covered system, a description of the reasons for not using such logical access controls or multifactor authentication.

D. A description of the following information security management practices used by the covered agency regarding covered systems:

    i. Policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

[2] A national security system, as defined in section 11103, title 40, United States Code, is a telecommunications or information system operated by the Federal Government that is used to support:

- intelligence activities;
- cryptologic activities related to national security;
- command and control of military forces;
- equipment that is an integral part of a weapon or weapons system; or
- military or intelligence missions.

[3] Logical access controls require users to authenticate themselves (through the use of passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions they can perform.

[4] Authentication is the process of verifying the identity of a user or verifying the source and integrity of data. The Act defines multifactor authentication as the use of not fewer than two authentication factors, such as:

- something that is known to the user, such as a password or personal identification number;
- an access device that is provided to the user, such as a cryptographic identification device or token; or
- a unique biometric characteristic of the user, such as fingerprints or face recognition.

[5] The Act defines covered agency as an agency that operates a covered system.

[6] The Act defines privileged user as a user who has access to system control, monitoring, or administrative functions.

ii. Capabilities the covered agency uses to monitor and detect data exfiltration and other threats, including:

I. data loss prevention[7] capabilities;

II. forensics[8] and visibility capabilities; or

III. digital rights management[9] capabilities.

iii. A description of how the covered agency is using the capabilities described in clause (ii).

iv. If the covered agency is not using capabilities described in clause (ii), a description of the reasons for not using such capabilities.

E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in (D).

[7] Data loss prevention is a system's ability to identify, monitor, and protect data in use, data in motion, and stored data through content inspection and security analysis of transactions. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of national security systems information.

[8] Forensics is the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

[9] Digital rights management is used to prevent unauthorized redistribution of digital media and restrict how information can be copied.

# Section 1

## Logical Access Controls

The Act defines logical access as a process of granting or denying specific requests to obtain and use information and related information-processing services. The Act requires the Inspector General of each covered agency to describe the agency's logical access policies and practices, list the logical access controls, and describe and list the multifactor authentication (a type of logical access control) used to govern system access by privileged users. In addition, the Act states that the Inspector General should determine whether the agency followed the policies.

### *Description of Logical Access Policies and Practices*

The DoD issued logical access policies, including policies requiring the use of multifactor authentication. Logical access controls require users to validate their identity through personal identification numbers, Common Access Cards,[10] biometric data, or security tokens.[11] The controls limit the files and resources users can access and the system actions they can perform. The DoD policies specifically describe logical access requirements related to identity authentication, public key infrastructure,[12] and securing unclassified, classified, and protected health information. The following DoD policies describe requirements for implementing logical access controls.

- *DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015.* The Instruction requires the DoD to grant access to electronic protected health information to personnel only on a need-to-know[13] basis. In addition, it requires personnel to have the appropriate clearance before accessing protected health information.
- *DoD Instruction 8500.01, "Cybersecurity," March 14, 2014.* The Instruction requires strong identification and authentication, including public key infrastructure, to be used for accessing DoD information systems.

[10] The DoD uses Common Access Cards to verify personal identity.

[11] A token is something that the individual possesses and controls (such as a key or password) that is used to authenticate a claim.

[12] Public key infrastructure is the framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates (a digitally signed representation of a user's identity).

[13] Need-to-know is a determination that a prospective recipient requires access to specific classified information in order to assist a government function.

- *DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012.* The Instruction requires unclassified DoD information possessed or controlled by non-DoD entities on non-DoD systems to be protected by at least one physical or electronic barrier, such as logical authentication.
- *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011 (current as of June 9, 2015).* The Instruction provides joint policy for information assurance and support to the DoD's computer network defense, which includes implementing security mechanisms to protect the DoD's computing environments. The Instruction requires using public key infrastructure to authenticate[14] identities, control access to DoD information systems,[15] and ensure confidentiality and integrity of DoD data, and nonrepudiation.[16] In addition, the Instruction requires that access to DoD information systems be granted only to individuals on a need-to-know basis. Furthermore, the Instruction requires users to change passwords every 60 days, be locked out of the network after three failed log-on attempts, and be logged out of the network after 15 minutes of inactivity. The Instruction also requires default passwords to be changed or removed, unique usernames and passwords to be used for group accounts, and expired accounts to be disabled or removed in a timely manner.
- *DoD Instruction 8520.02, "Public Key Infrastructure and Public Key Enabling," May 24, 2011.* The Instruction requires public key infrastructure to be implemented to control logical access to networks and systems through the use of Common Access Cards.
- *DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011.* The Instruction requires the use of Common Access Cards to access DoD information systems. The use of strong authentication[17] by using Common Access Cards helps prevent unauthorized individuals from exploiting compromised usernames and passwords.

[14] Authenticate means to confirm the identity of an individual or entity.

[15] An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[16] Nonrepudiation is the protection against an individual falsely denying having performed a particular action.

[17] Strong authentication requires two or more factors to securely authenticate a user. This includes something the user knows, such as a password; something the user is, such as physical characteristics or behavior traits; and something the user has, such as a security token.

~~(FOUO)~~ In addition to DoD-wide policies, the nine DoD Components issued policies that aligned with DoD requirements for logical access. For example, the Defense Human Resources Activity issued logical access control policies that require [redacted] The Defense Human Resources Activity also requires [redacted]

Furthermore, system owners[18] from the Defense Finance and Accounting Service (DFAS) and the Defense Information Systems Agency (DISA) issued policies that included logical access requirements specific to a covered system. For example, a DFAS policy[19] provides a standard framework for applying consistent logical access controls and processes for managing and controlling system access.

## *Description and List of Logical Access Controls*

DoD Instruction 8500.01[20] requires the DoD to implement system security controls designed by the National Institute of Standards and Technology (NIST).[21] NIST published a security controls catalog that provides guidelines for selecting and specifying controls based on risk. The nine DoD Components were required to use the catalog to identify specific security controls required for DoD systems and networks.[22] For example, DFAS system owners developed system security plans that included a list of the NIST security controls for logical access required to secure a specific system. Table 1 lists the broad categories of logical access controls included in the DFAS system security plans.

[18] Only DFAS and DISA provided both Component- and system-level policies and procedures. Therefore, references in this report to system owners pertain only to DFAS and DISA.

[19] DFAS Information and Technology Reference Document, "System Access Control," September 1, 2015.

[20] DoD Instruction 8500.01, "Cybersecurity," March 14, 2014.

[21] National Institute of Standards and Technology Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 (updated January 22, 2015).

[22] Although some DoD Components provided a list of logical access controls from an older DoD-specific system security control policy, DoD Information Assurance Certification and Accreditation Process, these controls align with the NIST requirements for logical access and multifactor authentication.

*Table 1. NIST SP 800-53 Logical Access Controls Implemented from the DFAS System Security Plans*

| Control Number | Control Name |
|---|---|
| AC-1 | Access Control Policy and Procedures |
| AC-2 | Account Management |
| AC-3 | Access Enforcement |
| AC-4 | Information Flow Enforcement |
| AC-5 | Separation of Duties |
| AC-6 | Least Privilege |
| AC-7 | Unsuccessful Log-on Attempts |
| AC-8 | System Use Notification |
| AC-10 | Concurrent Session Control |
| AC-11 | Session Lock |
| AC-12 | Session Termination |
| AC-14 | Permitted Actions Without Identification or Authentication |
| AC-17 | Remote Access |
| AC-18 | Wireless Access |
| AC-19 | Access Control for Mobile Devices |
| AC-20 | Use of External Information Systems |
| AC-21 | Information Sharing |
| AC-22 | Publicly Accessible Content |
| AT-3 | Security Training |
| PL-4 | Rules of Behavior |
| PS-3 | Personnel Screening |
| PS-4 | Personnel Termination |
| PS-5 | Personnel Transfer |
| PS-6 | Access Agreements |

## *Description and List of Multifactor Authentication Used to Govern Access to Covered Systems by Privileged Users*

System owners from DFAS and DISA provided policies that identified specific NIST security controls related to multifactor authentication for privileged users. For example, DFAS system owners developed system security plans that required implementing the NIST identification and authentication system control for organizational users. This control includes four control enhancements for privileged accounts.[23] Table 2 lists the four identification and authentication system control enhancements specific to privileged users.

*Table 2. NIST SP 800-53 Multifactor Authentication Controls for Privileged Users Implemented from the DFAS System Security Plans*

| Control Number | Control Name |
|---|---|
| IA-2 (1) | Network Access to Privileged Accounts |
| IA-2 (3) | Local Access to Privileged Accounts |
| IA-2 (6) | Network Access to Privileged Accounts – Separate Device |
| IA-2 (8) | Network Access to Privileged Accounts – Replay Resistant |

DoD Instruction 8520.02[24] requires DoD Components to use Common Access Cards for all users to access DoD networks and systems as a multifactor authentication control.[25] The nine DoD Components provided policies that described the use of Common Access Cards. However, DoD Instruction 8520.02 also allows DoD Components to request a waiver for using Common Access Cards when a system does not support public key infrastructure.[26]

[23] Privileged accounts are assigned to privileged users.

[24] DoD Instruction 8520.02, "Public Key Infrastructure and Public Key Enabling," May 24, 2011.

[25] In this report, the term users includes privileged users. Privileged users have trusted authorization to perform security-related functions on networks and systems not given to general users.

[26] Some DISA system owners provided public key infrastructure waivers.

## *Compliance with DoD Logical Access Policies and Practices*

Since FY 2013, the DoD audit community[27] has issued seven audit reports that concluded Components did not consistently follow logical access control requirements. The reports identified:

- inactive system accounts that were not properly managed within established timeframes;
- system accounts that were not removed when personnel no longer needed access;
- system access request forms that were missing or incomplete;
- system access request forms that did not provide sufficient justification to demonstrate the need for access to a DoD network or system; and
- shared or group system accounts that did not have unique usernames and passwords.

The DoD audit community generally identified that access control weaknesses existed because personnel did not follow existing policy. In the seven reports, the DoD audit community recommended, among other corrective actions, that DoD Components develop and implement specific controls, and update existing standard operating procedures. DoD Components generally agreed to implement the recommendations.

[27] The DoD audit community includes the DoD OIG, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency.

# Section 2

## Software Inventories and Licenses

The Act requires the Inspector General of the covered agency to describe the policies and procedures for conducting software and license inventories.

### *Description of Policies and Procedures for Conducting Software Inventories on Covered Systems*

The DoD issued policies that require system owners to conduct inventories of information resources,[28] information technology,[29] and assets,[30] all of which include software. The following DoD policies describe requirements for conducting software and software license inventories related to cybersecurity activities, information assurance, and computer network defense.

- *DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016.* The Instruction requires DoD Components to integrate cybersecurity activities to protect DoD information networks. It also requires an inventory of software applications to improve the effectiveness of conducting network operations and implementing internal defensive measures as part of a vulnerability management program.
- *DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014.* The Directive requires the DoD Chief Information Officer to maintain a current and complete inventory of the agency's information resources, which include software.
- *CJCSI 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011 (current as of June 6, 2015).* The Instruction requires DoD Components to establish and maintain a complete asset inventory of information resources. It also requires DoD Components to maintain a current and comprehensive baseline inventory of software and implement warning and tactical directives or orders that correspond to software within the Component's information technology resources and assets inventory.

[28] Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

[29] Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

[30] Assets include major applications (software programs), general support systems, high-impact programs, physical plants, mission-critical systems, personnel, equipment, or a logically related group of systems.

In addition to DoD-wide policies, six of the nine DoD Components issued policies and procedures that aligned with DoD requirements for conducting software inventories. For example, the Army issued policy that requires all Army commands to conduct an inventory of software products.[31] In addition, DFAS system owners provided system security plans that included system software baselines. System owners used the baselines to track and manage key software inventory items. Furthermore, the Missile Defense Agency (MDA) issued policy[32] requiring the Accountable Property Officer to manage and oversee assigned software and perform periodic inventories.

## *Description of Policies and Procedures for Conducting Inventories of Software Licenses*

~~(FOUO)~~ The DoD did not have policy for conducting software license inventories. However, Officials with the DoD Office of the Chief Information Officer stated that they are establishing an agencywide policy in response to a recommendation in the Government Accountability Office Report Number 14-413.[33] Although no DoD-wide policies or procedures existed that required software license inventories, three DoD Components issued policies and procedures on conducting software license inventories. For example, the Defense Information Systems Agency (DISA) issued procedures[34] that require each directorate to manage user software licenses. In addition, the Air Force requires organizations to maintain a software license inventory of government off-the-shelf and commercial off-the-shelf software.[35] Furthermore, the Navy issued policy[36] that requires [redacted]

[redacted]

[31] Memorandum for Multiple Enterprise License Agreement (ELA) Software Inventory Reporting, February 13, 2016.

[32] MDA Manual 4161.01-M, "MDA Property Accountability and Reporting," July 24, 2014.

[33] Government Accountability Office 14-413, "Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide," May 2014, reported that the DoD did not have an agencywide comprehensive policy for managing software licenses.

[34] Memorandum of Instructions to Request, Review, Validate, Approve/Deny, and Monitor DISA Standard and Non-Standard and Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) Software, February 26, 2016.

[35] Air Force Manual 33-153, "Information Technology (IT) Asset Management (ITAM)," March 19, 2014. Government-off-the-shelf refers to hardware and software products developed by the technical staff of a Government organization for use by the U.S. Government. Commercial-off-the-shelf refers to hardware and software products commercially made and available for sale, lease, or license to the general public.

[36] ~~(FOUO)~~ [redacted]

# Section 3

## Capabilities for Monitoring and Detecting Threats

The Act requires the Inspector General of each covered agency to describe capabilities that the agency uses to monitor and detect data exfiltration[37] and other threats, including these capabilities: (1) data loss prevention capabilities, (2) forensics and visibility capabilities, or (3) digital rights management capabilities. The Act also requires a description of how the capabilities are used, and if they are not being used, a description of the reasons.

### *Description of Capabilities Used to Monitor and Detect Threats*

In response to our request for data, all nine DoD Components reported using capabilities to monitor its networks and systems to detect threats and data exfiltration. The capabilities align with Federal and DoD requirements for detecting threats and data exfiltration attempts. Chairman of the Joint Chiefs of Staff Instruction 6510.01F[38] requires DoD Components to implement protection mechanisms such as firewalls, antivirus software, intrusion detection systems, and intrusion prevention systems to protect information systems. The DoD Component also reported the use of device control modules, data loss prevention tools, network analysis tools, and host[39]-based security systems (HBSS)[40] to monitor its networks and detect threats.

#### *Firewalls*

The DoD requires the use of firewalls as a boundary defense mechanism to monitor its networks and systems to prevent and detect malicious and unauthorized communications at the external perimeter of a network or system.[41] A firewall is a hardware and software capability that limits access between networks and systems in accordance with specific security policies. For example, the Navy requires network and system owners to configure firewalls to restrict network traffic and monitor system communications. The Defense Health Agency (DHA) also reported the use of firewalls to restrict access to known and approved communications.

---

37 Exfiltration is the unauthorized transfer of data from a computer.

38 CJCSI 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011.

39 A host is any hardware device that has the capability of permitting access to a network. Examples include, but are not limited to, computer and personal electronic devices.

40 HBSS capabilities provide a framework to implement a wide range of security solutions on hosts. The framework includes centralized management functions that provide automated protection to detect, respond, and report host-based vulnerabilities and incidents.

41 CJCSI 6510.01F, February 9, 2011.

### *Antivirus Software*

The DoD requires Components to implement virus protection such as antivirus tools to prevent and eliminate downloading, installing, and using unauthorized software on DoD networks. The DoD also requires Components to ensure antivirus software is installed on information systems used for accessing networks remotely.[42] DISA reported the use of the DoD's antivirus program to protect the DoD information network. The antivirus program includes real-time protection to secure systems from emerging threats. The MDA reported the use of antivirus software as a second layer of information security to protect systems from malware that could damage its networks. In addition, the Air Force requires the use of enterprise-wide tools such as antivirus software to prevent malware from operating on mobile computing devices that are not configured with antivirus software.

### *Intrusion Detection System*

The DoD requires information systems used for remote access to use host-based security, such as an intrusion detection system, before connecting to a remote access server. Intrusion detection is the process of monitoring events occurring on a computer system or network and analyzing them for signs of possible incidents. An intrusion detection system is software that automates the intrusion detection process. A host-based intrusion detection system can determine which processes and user accounts are involved in a cyberattack on the operating system. According to the Defense Human Resources Activity, managing its software is a primary goal of Component network monitoring and reporting. In addition, DISA reported the use of a network intrusion detection system to perform real-time traffic analysis on its networks. A network-based intrusion detection system detects attacks by capturing and analyzing network data. Furthermore, the DHA reported the use of a host-based intrusion detection system to protect system resources and applications from external and internal attacks. DFAS reported that it installed an automated host and network intrusion detection systems on all its networks and hosts.

[42] CJCSI 6510.01F, February 9, 2011.

### *Intrusion Prevention System*

The DoD requires its information systems to be monitored to detect intrusions that could threaten the security of DoD operations.[43] Intrusion prevention is the process of monitoring events occurring on a computer system or network, analyzing them for signs of possible incidents, and attempting to stop possible incidents. An intrusion prevention system is software that includes all the capabilities of an intrusion detection system as well as the ability to stop possible incidents. DFAS, for example, reported that it relies on intrusion protection system device alerts as a monitoring and detection resource. In addition, the DHA reported the use of a host-based intrusion prevention system to protect system resources and applications from external and internal attacks. According to the DHA's Concept of Operations,[44] intrusion prevention systems could also prevent unauthorized software from executing a cyberattack on networks.

### *Host-Based Security System*

~~(U//FOUO)~~ The DoD requires the use of DoD-provided, enterprise-wide automated tools such as HBSS to remediate vulnerabilities. HBSS capabilities provide a framework to implement security solutions on individual hosts. The framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond, and report host-based vulnerabilities and incidents. According to DISA, the primary goal of HBSS is to [redacted]

### *System Logs and Reviews*

The DoD requires its information systems to be monitored to detect intrusions, disruption of services, and unauthorized activities that could threaten the security of DoD operations.[45] System owners can use system logs to monitor and detect intrusions. System (or audit) logs are chronological records of system-generated activities that can identify who accessed the system and when, and the specific operations performed.[46] The DHA, for example, reported the use of system monitoring applications to log system activity. These applications can also identify malicious activity across its networks. The Defense Human Resources Activity reported the use of a log management tool to monitor system logs on a regular basis.

---

[43] CJCSI 6510.01F, February 9, 2011.

[44] DHA Network Operations Center Host Security Services (HSS) Concept of Operations (CONOPS), March 22, 2016.

[45] CJCSI 6510.01F, February 9, 2011.

[46] Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 6, 2015.

### *Network Analysis Tools*

~~(FOUO)~~ The DoD requires its information systems to be monitored to detect intrusions, disruption of services, and unauthorized activities that could threaten the security of DoD operations.[47] The DoD reported the use of network security analysis tools to collect, examine, and interpret network traffic to identify and respond to events that violate the security policy or posture of the resources attached to the network or the network infrastructure. For example, DISA reported the use of network analysis tools to [redacted][48] [redacted]. DISA also reported the use of network analysis tools for [redacted]

## *Description of Capabilities Used to Monitor and Detect Data Exfiltration*

### *Device Control Module*

As part of the DoD's incident response activities, DoD Components are required to prevent intruders from accessing or exfiltrating DoD data.[49] Network and system owners implemented the Device Control Module to monitor, control, and block external storage devices and peripheral ports. A Device Control Module prevents data loss and data leaks, and ensures compliance with security settings while also preventing the spread of malware and viruses. For example, DISA reported the use of a Device Control Module to disable write privileges on removable media devices for classified servers, systems, and workstations. The Marine Corps reported the use of a Device Control Module as part of its HBSS, and the DHA reported the use of a Device Control Module to monitor attempts to copy data to removable media.

### *Data Loss Prevention Tools*

The DoD information systems are required to be monitored to detect and react to incidents related to unauthorized activity.[50] Data loss is confidential or private information leaving the enterprise because of unauthorized communications through applications, physical devices, or network protocols. Data loss prevention capabilities detect and prevent the unauthorized use and transmission of national security system information. The MDA, for example, reported the use of data loss prevention tools to deny users access to prohibited sites, such as file sharing or storage sites, that could be used to knowingly or unknowingly share sensitive

[47] CJCSI 6510.01F, February 9, 2011.
[48] Denial of service prevents authorized access to resources or delays time-critical operations.
[49] Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," July 10, 2012.
[50] CJCSI 6510.01F, February 9, 2011.

information. The MDA also reported the use of HBSS as a data loss prevention tool to disable, enable, and monitor removable media.[51] The Marine Corps reported the use of data loss prevention software to protect the Marine Corps Enterprise Network from unauthorized data transfers.

[51] Removable media are a portable data storage media such as compact discs, flash memory devices, or external hard drives that can be added to or removed from a computing device or network.

# Section 4

## Third-Party Service Providers

The Act requires the Inspector General of each covered agency to describe policies and procedures that ensure entities providing the DoD with services (third-party service providers) implement information security management practices, such as conducting software and license inventories, and using capabilities to monitor and detect data exfiltration and threats.

### *Description of Policies for Ensuring Third-Party Service Providers Implement Information Security Management Practices*

The DoD issued policies that require cybersecurity service providers to implement computer network defense to monitor and detect data exfiltration and cyber threats. Computer network defense includes actions—such as monitoring, detecting, analyzing, responding, and restoring activities—that defend against unauthorized activity within a network. The following DoD policies describe third-party service provider requirements for implementing information security management practices.

- *Defense Federal Acquisition Regulation Supplement, Section 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," May 2016.* The Regulation requires DoD contractors to implement information systems security protections to provide adequate security on all contractor information systems.
- *DoD Cybersecurity Discipline Implementation Plan (the Plan), October 2015 (amended February 2016).* The DoD issued the Plan to reinforce basic cybersecurity requirements identified in policies, directives, and orders. The Plan aligns cybersecurity with computer network defense service providers to improve the detection of and response to cyber threats. According to the Plan, monitoring activities ensure DoD rapidly identifies and responds to potential threats.
- *Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," July 10, 2012.* This Manual requires third parties that provide computer network defense services to monitor, analyze, and detect network threats. The Manual also describes a process for reporting incidents to affected DoD installations.

- ~~(FOUO)~~ *DoD O-8530.1-M Program Manual, "Department of Defense Computer Network Defense Service Provider Certification and Accreditation Process," December 17, 2003.* The Manual [redacted]

## *Description of Procedures for Ensuring Third-Party Service Providers Use Monitoring and Detecting Capabilities*

Seven of the nine DoD Components provided details for ensuring third-party service providers use monitoring and detecting capabilities. DoD Components also developed procedures that aligned with the DoD requirement to ensure third-party service providers use capabilities to monitor and detect cyber threats and data exfiltration. For example, the DHA issued standard operating procedures[52] to establish specific responsibilities for third-party service providers. Specifically, the standard operating procedures require computer network defense service providers to maintain an HBSS to monitor, detect, and defend DoD networks and systems. In addition, the DHA requires third-party service providers to use remote forensics and threat analysis tools to identify suspicious cyber events.

## *Description of Procedures for Ensuring Third-Party Service Providers Conduct Inventories of Software and Licenses*

The DoD Chief Information Officer did not issue specific DoD-wide policy for ensuring third-party service providers conducted software and associated license inventories. However, one DoD Component issued policy for conducting software and license inventories used by third-party providers. Specifically, in DISA's performance work statements for third-party service providers, DISA requires that the third-party service providers conduct software inventories and maintain software inventory lists. DISA also requires third-party service providers to conduct an inventory to maintain accountability for software and associated licenses.

[52] DHA "Network Security Operations Branch Connection Approval Process Standard Operating Procedure," March 2016.

# Appendix A

## Scope and Methodology

We conducted this summary work from March 2016 through August 2016. This report summarizes policies and procedures obtained from the DoD Chief Information Officer and nine DoD Components[53] through a request for data. Although announced as an assessment, we did not conduct an audit, assessment, or evaluation in accordance with applicable standards. We did, however, perform this effort in accordance with applicable standards of the Council of Inspectors General on Integrity and Efficiency, "Quality Standards for Federal Offices of Inspector General," August 2012. We identified recommendations from previous audits. Therefore, this report contains no new recommendations and is provided for information purposes only.

To address the Act's requirements, we contacted the DoD Chief Information Officer, as well as the nine Components listed in Table 3, and requested policies and procedures related to logical access, software inventories, threat detection capabilities, and services provided by third parties. We did not independently verify, analyze, or validate information provided from the DoD Components.

~~(FOUO)~~ Based on a March 15, 2016, report from the Defense Information Technology Portfolio Repository, the DoD maintained [redacted] systems, of which [redacted] were covered systems. Of the [redacted] covered systems, [redacted] systems were identified as national security systems and [redacted] systems were identified as having access to personally identifiable information. Nine DoD Components maintained [redacted] of the systems, to include [redacted] percent of the national security systems ([redacted] systems) and [redacted] percent of the systems containing personally identifiable information ([redacted] systems). (See Table 3.)

[53] Although the DoD Chief Information Officer does not own systems that fall within the parameters of the Act, the office develops information technology, information management, and cybersecurity policies for the Department. References in this report to the nine Components refer to the nine Components that manage covered systems, and not to the DoD Chief Information Officer.

*Table 3. DoD Components That Manage National Security Systems and Systems With Access to Personally Identifiable Information*

| ~~(FOUO)~~ DoD Component | National Security Systems | Systems With Access to Personally Identifiable Information |
|---|---|---|
| Army | [redacted] | [redacted] |
| Marine Corps | [redacted] | [redacted] |
| Navy | [redacted] | [redacted] |
| Air Force | [redacted] | [redacted] |
| Defense Finance and Accounting Service | [redacted] | [redacted] |
| Defense Information Systems Agency | [redacted] | [redacted] |
| Defense Health Agency | [redacted] | [redacted] |
| Defense Human Resources Activity | [redacted] | [redacted] |
| Missile Defense Agency | [redacted] | [redacted] |
| **Totals** | [redacted] | [redacted] ~~(FOUO)~~ |

In response to our request for data (see Appendix B), we received DoD-wide policies as well as Component-level, and system-level policies and procedures from the nine Components. After receiving and reviewing more than 775 policies and procedures, we determined that DoD Components issued 339 policies and procedures[54] related to logical access, software inventory, monitoring and detecting threats, and third-party service providers. (See Appendix C for a list of relevant policies and procedures.)

We contacted the DoD Service audit agencies[55] and requested audit reports on DoD Components that did not follow policies and procedures related to logical access. We also identified Department of Defense Inspector General (DoD IG) audit reports on DoD Components that did not follow logical access policies and procedures. We received and reviewed more than 33 audit reports from FY 2013 to FY 2016, and identified 7 audit reports that discussed noncompliance with logical access control requirements. (See Appendix D for a list of the seven audit reports.)

[54] Policies and procedures addressed multiple information security management categories (logical access, software and license inventories, and third-party service providers).

[55] The DoD Service audit agencies are the Army Audit Agency, Naval Audit Service, and the Air Force Audit Agency.

## Use of Computer-Processed Data

The DoD OIG used the Defense Information Technology Portfolio Repository to generate a list of the DoD's national security systems and systems with access to personally identifiable information. The Defense Information Technology Portfolio Repository is the DoD's official unclassified registry and data source for the inventory of mission-critical, mission-essential, and mission support systems.

# Appendix B

## Data Request

**Attachment**

Page 1 of 2

The Cybersecurity Act of 2015 (the Act) was enacted on December 18, 2015. The Act includes a requirement for Federal Inspectors General to generate a report describing agency policies, procedures, and practices for "covered systems." The Act describes covered systems as national security systems as defined in section 11103, title 40, United States Code, and Federal computer systems that provide access to personally identifiable information. The report is to be submitted to the agency committees of jurisdiction in the Senate and House of Representatives within 240 days of enactment of the Act.

1. The Act states that the report contents should include the following:

**A. Logical Access Controls**

- Description of logical access policies and practices used to access a covered system.
- Description and list of logical access controls and multifactor authentication used to govern access to covered systems by privileged users.
- Description of the reasons for not using logical access controls or multifactor authentication, if applicable.
- Assessment of whether logical access policies and practices were followed.

**B. Software Inventories and Licenses**

Description of policies and procedures followed to conduct inventories of the software present on covered systems and the licenses associated with the software.

**C. Monitoring and Detecting Exfiltration and Other Threats**

- Description of capabilities used to monitor and detect threats, including data loss prevention, forensics and visibility capabilities, or digital rights management.
- Description of how agencies are using the capabilities.
- Description of reasons for not using these capabilities, if applicable.

**D. Contractor and Other Entities**

Description of the policies and procedures with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing controls for conducting software and license inventories, and monitoring and detecting exfiltration and other threats.

2. According to the Defense Information Technology Portfolio Repository (DITPR), as of March 1, 2016, DoD maintains 6,174 systems. Of the 6,174 systems listed in DITPR, 2,809 systems meet the Act's definition of a covered system. Specifically, 1,720 are listed as national security systems and 1,089 are listed as non-national security systems that contain personally identifiable information.

Attachment

# Data Request (cont'd)

**Attachment (cont'd)**

Page 2 of 2

3. In support of the Act's requirements, we request the following information be sent to CSA2015@dodig.mil by April 22, 2016:

A. logical access policies and practices used to access a covered system.
B. logical access controls and multifactor authentication used to govern access to covered systems by privileged users.
C. policies and procedures for conducting inventories of the software on covered systems, and the licenses associated with the software.
D. capabilities used to monitor and detect exfiltration and other threats, including:
    a. data loss prevention capabilities;
    b. forensics and visibility capabilities; and
    c. digital rights management capabilities.
E. a description of how the agency is using the capabilities listed in 3.D above.
F. policies and procedures to ensure that entities, including contractors, that provide services to the agency are implementing the information security management practices listed in 3.D above.

Attachment

# Appendix C

## Relevant Information Security Management Policies and Procedures

*Table 4. Federal/Overall DoD*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | DoD Instruction 8530.01, Cybersecurity Activities Support to DoD Information Network Operations | March 7, 2016 | X | X | X | |
| 2 | DoD Cybersecurity Discipline Implementation Plan | October 2015 | X | | X | |
| 3 | DoD Instruction 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs | August 12, 2015 | X | | X | X |
| 4 | ~~(U//FOUO)~~ [redacted] | July 5, 2015 | x | | | |
| 5 | DoD Instruction 8540.01, Cross Domain (CD) Policy | May 8, 2015 | | X | | |
| 6 | DoD Directive 5144.02, DoD Chief Information Officer (DoD CIO) | November 21, 2014 | X | X | | |
| 7 | DoD Directive 5400.11, DoD Privacy Program | October 29, 2014 | | | | X |
| 8 | DoD Directive 5205.16, The DoD Insider Threat Program | September 30, 2014 | | | | X |
| 9 | DoD Instruction 8551.01, Ports, Protocols, and Services Management (PPSM) | May 28, 2014 | X | | | |
| 10 | DoD Instruction 8500.01, Cybersecurity | March 14, 2014 | X | | | X |
| 11 | DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) | March 12, 2014 | X | | | X |
| 12 | DoD Directive 5240.06, Counterintelligence Awareness and Reporting | May 30, 2013 | | | | X |
| 13 | National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations | April 2013 | X | | | |
| 14 | DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities | September 11, 2012 | X | | | ~~(FOUO)~~ |

Table 4 legend is located on the final table page.

*Table 4. Federal/Overall DoD (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 15 | Chairman of the Joint Chiefs of Staff Instruction 6510.01B, Cyber Incident Handling Program | July 10, 2012 | | | | X |
| 16 | DoD Instruction 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems | June 6, 2012 | X | | | |
| 17 | DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling | May 24, 2011 | X | | | |
| 18 | DoD Instruction 8520.03, Identity Authentication for Information Systems | May 13, 2011 | X | | | |
| 19 | DoD Instruction 5220.22, National Industrial Security Program (NISP) | March 18, 2011 | | | | X |
| 20 | Chairman of the Joint Chiefs of Staff Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND) | February 9, 2011 | X | X | X | X |
| 21 | DoD Instruction 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense | June 8, 2010 | | | | X |
| 22 | DoD Instruction 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing | October 9, 2007 | | | X | |
| 23 | DoD 5220.22-M, National Industrial Security Program Operating Manual | February 28, 2006 | X | | | |
| 24 | ~~(U//FOUO)~~ [redacted] | December 17, 2003 | | | | X |
| 25 | Defense Federal Acquisition Regulation Supplement - Part 252, Solicitation Provisions and Contract Clauses | May 10, 2016 | | | | X ~~(FOUO)~~ |

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 5. Army*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | Army Information Security Management Practices | *April 22, 2016* | | | X | |
| 2 | Multiple Enterprise License Agreement (ELA) Software Inventory Reporting | February 13, 2016 | | X | | |
| 3 | Procedures for Conducting Software and License Inventory | *April 22, 2016* | | X | | |
| 4 | Privileged Users Authentication Requirements | April 15, 2016 | X | | | |
| 5 | Information Paper: New Army Training and Certification Tracking System (ATCTS) Feature for the New DoD Directive 8140.01, DoD Cyberspace Workforce Framework (DCWF) Initiative | February 1, 2016 | X | | | |
| 6 | ~~(U//FOUO)~~ [redacted] | February 2016 | X | | | |
| 7 | Privileged/Elevated Access to Army Information Systems, Networks and Data | January 26, 2016 | X | | | |
| 8 | Army Regulation 25-1, Army Information Technology | June 25, 2013 | X | | X | |
| 9 | Army Regulation 380-53, Communications Security Monitoring | January 17, 2013 | | | X | |
| 10 | Army Regulation 25-2, Information Assurance | March 23, 2009 | X | | X | ~~(FOUO)~~ |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 6. Marine Corps*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | ~~(U//FOUO)~~ [redacted] | *April 26, 2016* | X | | | |
| 2 | ~~(FOUO)~~ [redacted] | February 2016 | X | | | |
| 3 | ~~(FOUO)~~ [redacted] | February 2016 | X | | | |
| 4 | Marine Corps Order 5239.2B: Marine Corps Cybersecurity | November 5, 2015 | X | | X | |
| 5 | ~~(FOUO)~~ [redacted] | September 15, 2015 | X | | | |
| 6 | ~~(FOUO)~~ [redacted] | September 2015 | X | | | |
| 7 | ~~(U//FOUO)~~ [redacted] | September 2015 | | | X | |
| 8 | Operation Order (OPORD) 15-0001 - Marine Corps Command Cyber | September 2015 | X | | X | |
| 9 | ~~(U//FOUO)~~ [redacted] | December 2014 | | | X | |
| 10 | ~~(U//FOUO)~~ [redacted] | October 2014 | | | X | |
| 11 | ~~(U//FOUO)~~ [redacted] | July 2014 | | | X | |
| 12 | ~~(U//FOUO)~~ [redacted] | May 2014 | X | | | ~~(FOUO)~~ |

Table 6 legend is located on the final table page.

*Table 6. Marine Corps (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 13 | ~~(U//FOUO)~~ [redacted] | March 2014 | X | | | |
| 14 | ~~(U//FOUO)~~ [redacted] | February 2014 | | | X | |
| 15 | ~~(FOUO)~~ [redacted] | December 31, 2013 | | | X | |
| 16 | ~~(FOUO)~~ [redacted] | December 1, 2013 | X | | | |
| 17 | ~~(FOUO)~~ [redacted] | October 15, 2012 | | | X | |
| 18 | ~~(FOUO)~~ [redacted] | August 8, 2012 | | | X | |
| 19 | ~~(FOUO)~~ [redacted] | June 11, 2012 | X | | X | |
| 20 | ~~(FOUO)~~ [redacted] | May 15, 2012 | | | X | |
| 21 | ~~(FOUO)~~ [redacted] | September 30, 2011 | X | | X | |
| 22 | ~~(FOUO)~~ [redacted] | September 15, 2011 | X | | | ~~(FOUO)~~ |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

The Marine Corps provided the audit team with 23 relevant documents labeled Secret. These documents are not included in this appendix.

*Table 7. Navy*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | Director, Department of the Navy, Deputy Chief Information Officer (Navy) (DDCIO(N)) Memorandum, Guidance on Selecting Non-PKI Based Multi-Factor User Authentication | March 28, 2016 | X | | | |
| 2 | Director, Department of the Navy, Deputy Chief Information Officer (Navy) (DDCIO(N)) Memorandum, Enforcement of Cryptographic Logon | March 23, 2016 | X | | | |
| 3 | NAVADMIN 028/16, Public Key Infrastructure Enforcement on Navy Nonsecure Internet Protocol Router Network and Secret Internet Protocol Router Network | February 2016 | X | | | |
| 4 | ~~(U//FOUO)~~ [redacted] | January 15, 2016 | X | X | X | X |
| 5 | ~~(U//FOUO)~~ [redacted] | October 26, 2015 | X | | X | |
| 6 | ~~(U//FOUO)~~ [redacted] | September 14, 2015 | | | X | |
| 7 | ~~(U//FOUO)~~ [redacted] | June 18, 2015 | X | | X | |
| 8 | ~~(U//FOUO)~~ [redacted] | May 6, 2015 | | | X | |
| 9 | ~~(U//FOUO)~~ [redacted] | May 6, 2015 | | | X | |
| 10 | ~~(U//FOUO)~~ [redacted] | January 27, 2015 | X | | X | |
| 11 | ~~(U//FOUO)~~ [redacted] | January 27, 2015 | X | | X | ~~(FOUO)~~ |

Table 7 legend is located on the final table page.

*Table 7. Navy (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 12 | ~~(U//FOUO)~~ [redacted] | January 27, 2015 | | | X | |
| 13 | Secretary of the Navy Instruction 2075.1, Department of the Navy Commercial Wireless Local Area Network (WLAN) Devices, Services, and Technologies | November 30, 2006 | X | | X | ~~(FOUO)~~ |

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 8. Air Force*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | AFMAN 33-153, Information Technology (IT) Asset Management (ITAM) | March 19, 2014 | | X | | |
| 2 | Air Force Manual 33-152, User Responsibilities and Guidance for Information | June 1, 2012 | X | | | |
| 3 | Air Force Manual 33-282, Computer Security (COMPUSEC) | March 28, 2012 | X | | X | |
| 4 | Air Force Instruction 33-210, Air Force Certification and Accreditation (C&A) Program | December 23, 2008 | | | | X ~~(FOUO)~~ |

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 9. Defense Information Systems Agency*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 2 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 3 | Memorandum for Program Executive Officer for Command and Control Capabilities, DAA Acceptance of Risk (DRA) for U.S. PKI/PKE Non-Implementation on DISA Supported CENTRIXS Network Pods | *April 25, 2016* | X | | | |
| 4 | Procedures for DCI | *April 25, 2016* | X | X | X | X |
| 5 | Procedures for WhiteList Tool Network | *April 25, 2016* | X | X | X | |
| 6 | Procedures for CENTRIXS | *April 25, 2016* | X | X | X | |
| 7 | Procedures for Computer Services Division Operations Denver | *April 25, 2016* | X | X | X | |
| 8 | Procedures for DECC Pacific | *April 25, 2016* | X | X | X | X |
| 9 | Procedures for Global Management Center | *April 25, 2016* | X | X | X | |
| 10 | Procedures for NCCS | *April 25, 2016* | X | X | X | |
| 11 | ~~(U//FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 12 | Multi-National Information Sharing (MNIS) Combined Federated Battle Lab Network (CFBLNET) Performance Work Statement (PWS) | *April 22, 2016* | | | | X |
| 13 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 14 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 15 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 16 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X ~~(FOUO)~~ |

Table 9 legend is located on the final table page.

*Table 9. Defense Information Systems Agency (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 17 | ~~(FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 18 | ~~(U//FOUO)~~ [redacted] | *April 22, 2016* | | | X | |
| 19 | Procedures for Defense Collaboration Services | *April 22, 2016* | X | X | X | |
| 20 | Performance Work Statement for Multi-National Information Sharing (MNIS), Design, Transition, and Operation (DTO) Support Services | *April 22, 2016* | | | | X |
| 21 | Procedures for Enterprise Email Security Gateway | *April 22, 2016* | X | X | X | X |
| 22 | ~~(U//FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 23 | ~~(U//FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X |
| 24 | Procedures for JSC Enclave | *April 25, 2016* | X | X | X | |
| 25 | Procedures for Tactical Data Link Document System (TDS-C) | *April 22, 2016* | X | X | X | X |
| 26 | Procedures for Web Content Filter | *April 22, 2016* | X | X | X | X |
| 27 | Procedures for CFBLNet | *April 22, 2016* | X | X | X | X |
| 28 | Procedures for Joint Communications Simulation System (JCSS) | *April 22, 2016* | X | X | X | X |
| 29 | Procedures for Pegasus | *April 22, 2016* | X | X | X | X |
| 30 | Procedures for Cross Domain Enterprise Solution | *April 22, 2016* | X | X | X | X |
| 31 | Procedures for SABER | *April 21, 2016* | X | X | X | |
| 32 | ~~(U//FOUO)~~ [redacted] | *April 22, 2016* | X | X | X | X ~~(FOUO)~~ |

Table 9 legend is located on the final table page.

*Table 9. Defense Information Systems Agency (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 33 | Procedures for Mobility Account Manager | *April 25, 2016* | X | X | X | |
| 34 | Procedures for Newton | *April 21, 2016* | X | X | X | |
| 35 | Procedures for CAWSN | *April 21, 2016* | X | X | X | |
| 36 | AntiDrug Network (ADNET) Access Control Assessment | April 25, 2016 | X | | | |
| 37 | ~~(U//FOUO)~~ [redacted] | *April 20, 2016* | | | | X |
| 38 | DISA Memorandum of Agreement (MOA) between DoD Teleport Program Office and DISA CONUS Global NETOPS Support Center on Teleport Limited Internet Protocol (IP) System Management | June 27, 2005 | | | | X |
| 39 | Procedures for DoD Teleport | April 20, 2016 | X | X | X | X |
| 40 | Procedures for ADNET-S | April 19, 2016 | X | X | X | X |
| 41 | ~~(FOUO)~~ [redacted] | April 18, 2016 | X | | | |
| 42 | ~~(U//FOUO)~~ [redacted] | March 10, 2016 | | X | | |
| 43 | ~~(FOUO)~~ [redacted] | March 7, 2016 | X | | | |
| 44 | Memorandum of Instructions to Request, Review, Validate, Approve/Deny, and Monitor DISA Standard and Non-Standard and GOTS or COTs Software | February 26, 2016 | | X | | |
| 45 | ~~(U//FOUO)~~ [redacted] | February 22, 2016 | X | | | |
| 46 | ~~(U//FOUO)~~ [redacted] | February 22, 2016 | X | | | |
| 47 | ~~(U//FOUO)~~ [redacted] | *February 2, 2015* | | X | | |
| 48 | ~~(U//FOUO)~~ [redacted] | January 2016 | X | | X | |
| 49 | ~~(U//FOUO)~~ [redacted] | December 22, 2015 | X | | | ~~(FOUO)~~ |

Table 9 legend is located on the final table page.

*Table 9. Defense Information Systems Agency (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 50 | ~~(U//REL to AUS/CAN/NZ/UK/US~~ [redacted] | December 21, 2015 | X | | | |
| 51 | ~~(FOUO)~~ [redacted] | December 19, 2015 | X | | | |
| 52 | ~~(U//FOUO)~~ [redacted] | *December 17, 2015* | X | | | |
| 53 | ~~(U//FOUO)~~ [redacted] | November 16, 2015 | X | | | |
| 54 | ~~(U//FOUO)~~ [redacted] | September 28, 2015 | X | | | |
| 55 | ~~(FOUO)~~ [redacted] | September 25, 2015 | | X | | |
| 56 | DISA Memorandum, DoD Teleport Waiver for Two-Factor Authentication Requirement | June 23, 2015 | X | | | |
| 57 | ~~(FOUO)~~ [redacted] | May 27, 2015 | | | X | |
| 58 | Two-Factor Authentication (DISA OPORD 15-001), Waiver Request for Select Components of the DoD Teleport System | June 23, 2015 | X | | | |
| 59 | ~~(U//FOUO)~~ [redacted] | April 24, 2015 | | | X | |
| 60 | ~~(U//FOUO)~~ [redacted] | March 25, 2015 | X | X | X | |
| 61 | Memorandum for DISA Authorizing Official (AO), Non-Compatible Host-Based Security Systems (HBSS) Assets in the DoD Enterprise Classified Travel Kit - Gateway (DECTK-GW) | March 18, 2015 | | | X | ~~(FOUO)~~ |

Table 9 legend is located on the final table page.

*Table 9. Defense Information Systems Agency (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 62 | Access Control Policy and Procedures for National Military Command Center (NMCC), Command and Control System (NCCS) | March 17, 2015 | X | | | |
| 63 | ~~(U//FOUO)~~ [redacted] | March 10, 2015 | | | X | |
| 64 | Antidrug Network Program (ADNET), Performance Work Statement | September 22, 2014 | | | | X |
| 65 | Riverbed Contract with Performance Work Statement for Joint Communications Simulation System (JCSS) | August 26, 2014 | | | | X |
| 66 | Reference Standard Operating Procedures (SOP) 310-240-12, Computer Network Defense Service Provider, ESD Net Assurance, Tactics, Techniques, and Procedures | January 16, 2014 | | | X | |
| 67 | ~~(U//FOUO)~~ [redacted] | September 27, 2013 | | | X | |
| 68 | ~~(U//FOUO)~~ [redacted] | August 15, 2013 | X | | | |
| 69 | ~~(U//FOUO)~~ [redacted] | July 2011 | X | | X | ~~(FOUO)~~ |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 10. Defense Finance and Accounting Service*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | ~~(U//FOUO)~~ [redacted] | May 2016 | X | | X | X |
| 2 | Human Resources Business Intelligence Dashboard (HRBID) Audit Log Checks | *April 22, 2016* | | | X | |
| 3 | Automated Disbursing System (ADS) 3801 - Centralized Disbursing System (CDS) | *April 22, 2016* | X | | | X |
| 4 | Information Security Policy (provided with 1099 TRP documents) | *April 22, 2016* | X | | | |
| 5 | ePortal System Logging Procedures | *April 22, 2016* | | | X | |
| 6 | 1099 Tax Reporting Program (1099TRP), Security Rules of Behavior (SROB) | *April 22, 2016* | X | | | |
| 7 | DFAS Security Control Baseline, Automated Time Attendance and Production System | *April 21, 2016* | X | | | |
| 8 | Defense Military Pay Office (DMO) System, Application Log Review Procedure | *April 20, 2016* | | | X | |
| 9 | Audit Logging Procedures for Defense Debt Management System (DDMS) | *April 20, 2016* | | | X | |
| 10 | Procedures for Defense Corporate Database/Defense Corporate Warehouse (DCD/DCW) DITPR 17250 | *April 20, 2016* | X | X | | |
| 11 | DFAS Security Control Baseline, Integrated Automated Travel System | *April 20, 2016* | X | | | |
| 12 | Defense MilPay Office DFAS MilPay Repository (DMO/DMR) Access Control Plan | *April 20, 2016* | X | | | |
| 13 | ~~(FOUO)~~ [redacted] | *April 19, 2016* | X | | | X ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 14 | ~~(U//FOUO)~~ [redacted] | *April 19, 2016* | X | | | |
| 15 | FY 2015-2017 Interservice Support Agreement (ISA) for STARS System Support provided by Naval Supply Systems Command (NAVSUP) Business Systems Center to Defense Finance and Accounting Service (DFAS) | *April 19, 2016* | | | | X |
| 16 | Auditing, Logging and Monitoring of Defense Finance and Accounting Service (DFAS) Systems | *April 18, 2016* | | | X | |
| 17 | DFAS Access Control Policy for Integrated Garnishment System (IGS) | *April 18, 2016* | X | | | |
| 18 | ~~(FOUO)~~ [redacted] | April 12, 2016 | X | | | |
| 19 | DFAS Security Control Baseline, Deployable Disbursing System (DDS) | April 6, 2016 | X | X | | |
| 20 | System Access Control Policy for Operational Data Store (ODS) | April 2016 | X | | | |
| 21 | ~~(FOUO)~~ [redacted] | April 2016 | X | | | |
| 22 | ~~(U//FOUO~~ [redacted] | April 2016 | X | | X | |
| 23 | Defense Business Management, System Access Control Policy (ACP) | March 30, 2016 | X | | | |
| 24 | ~~(FOUO)~~ [redacted] | March 23, 2016 | X | | | |
| 25 | System Security Plan (SSP) Template for Defense Retiree and Annuitant Payroll System | March 23, 2016 | X | | | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 26 | System Security Plan (SSP) for Defense Finance and Accounting Services (DFAS) Enterprise Local Area Network (ELAN) | March 22, 2016 | X | X | X | |
| 27 | System Security Plan for Automated Disbursing System 3801, Centralized Disbursing System (CDS) | March 18, 2016 | X | | X | |
| 28 | I&T Shared Services, DFAS Corporate Database (DCD) Database Administrator (DBA) Audit Log Review Procedures | March 18, 2016 | X | | X | |
| 29 | Standard Accounting and Reporting System (STARS), Access Control Policy | March 11, 2016 | X | | | |
| 30 | ~~(FOUO)~~ [redacted] | March 8, 2016 | X | | | |
| 31 | System Security Plan for the Case Management System | March 8, 2016 | X | | X | |
| 32 | ~~(U//FOUO)~~ [redacted] | March 2016 | X | | X | |
| 33 | Defense Civilian Pay System (DCPS), Security Standard Operating Procedures (SSOP) | March 2016 | X | | X | |
| 34 | System Security Plan (SSP) for Business Continuity Planning System (BCPS) | March 2016 | X | | | |
| 35 | Standard Accounting, Budgeting, and Reporting System (SABRS), Access Control Policy | March 2016 | X | | | |
| 36 | Standard Negotiable Instrument Processing System (SNIPS) | March 2016 | X | | | |
| 37 | System Security Plan (SSP) for Electronic Document Management (EDM) | March 2016 | X | | X | |
| 38 | ~~(FOUO)~~ [redacted] | March 2016 | X | | | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 39 | ~~(FOUO)~~ [redacted] | March 2016 | | | | X |
| 40 | ~~(FOUO)~~ [redacted] | March 2016 | | | | X |
| 41 | Information System Contingency Plan (ISCP), Electronic Document Management (EDM) | March 2016 | | X | X | X |
| 42 | ~~(U//FOUO)~~ [redacted] | March 2016 | X | | | |
| 43 | Integrated Automated Travel System (IATS), System Access Control Policy (SACP), and Standard Operating Procedures (SOP) | February 23, 2016 | X | | | |
| 44 | Procedures for Initial Access to Automated Disbursing System (ADS) | February 16, 2016 | X | | | |
| 45 | Deployable Disbursing System (DDS), Application Audit Logging and Monitoring Policy and Procedures | February 5, 2016 | | | X | X |
| 46 | ~~(FOUO)~~ [redacted] | February 3, 2016 | X | | | |
| 47 | ~~(FOUO)~~ [redacted] | February 2016 | X | | | |
| 48 | ~~(FOUO)~~ [redacted] | January 29, 2016 | X | | | |
| 49 | ~~(FOUO)~~ [redacted] | January 28, 2016 | X | | | |
| 50 | DFAS-Indianapolis Operations Standard Finance System Procedures Accounting Operation Systems Office | January 26, 2016 | X | | | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 51 | Deployable Disbursing System, System Security Plan (SSP) | January 15, 2016 | X | | | |
| 52 | System Security Plan (SSP) for Standard Finance System | January 2016 | | X | | X |
| 53 | System Access Control Policy for Standard Operations and Maintenance, Army Research and Development System (SOMARDS) | January 2016 | X | | | |
| 54 | System Access Controls, One Pay | January 2016 | X | | | |
| 55 | Defense Working Capital Fund (DWCF) Services, Service Level Agreement (SLA) between Defense Information Systems Agency (DISA) and Defense Finance and Accounting Service (DFAS) | December 21, 2015 | | | | X |
| 56 | DFAS-Japan Operations, Standard Finance System Procedures | December 14, 2015 | X | | | |
| 57 | ~~(FOUO)~~ [redacted] | December 9, 2015 | X | | | |
| 58 | Consolidated Returned Item Stop-Payment System (CRISPS) | December 2015 | X | | | |
| 59 | ~~(FOUO)~~ [redacted] | December 1, 2015 | | | | X |
| 60 | System Access Control Policy and Standard Operating Procedures for DFAS 1099 Tax Reporting Program | November 23, 2015 | X | | | |
| 61 | Defense Working Capital Fund Accounting System (DWAS), Access Control Policy | November 10, 2015 | X | | | |
| 62 | DFAS Instruction 8510.01-I, Risk Management Framework | November 10, 2015 | X | | | X |
| 63 | System Security Plan (SSP) for Human Resources Information System (HRIS) | November 2, 2015 | X | | X | |
| 64 | System Security Plan (SSP) for Operational Data Store (ODS) | October 27, 2015 | X | X | X | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 65 | ~~(FOUO)~~ [redacted] | October 21, 2015 | X | | | X |
| 66 | ~~(FOUO)~~ [redacted] | October 20, 2015 | X | | | |
| 67 | System Security Plan (SSP) for Standard Accounting and Reporting System (STARS) | October 16, 2015 | X | X | | |
| 68 | ~~(FOUO)~~ [redacted] | October 2015 | | | | X |
| 69 | Security Procedure Guide for Standard Operations & Maintenance, Army Research & Development System | October 2015 | X | | | |
| 70 | System Security Plan (SSP) for Defense MilPay Office DFAS MilPay Repository (DMO/DMR) Client Server and Web Applications | October 2015 | X | | | |
| 71 | System Security Plan (SSP) for Integrated Automated Travel System (IATS) | October 2015 | X | X | | |
| 72 | System Security Plan (SSP), Defense Joint Military Pay System (DJMS) | September 9, 2015 | X | | | |
| 73 | System Security Plan (SSP) for Integrated Accounts Payable System (IAPS) | September 2015 | X | | | |
| 74 | System Access Controls | September 1, 2015 | X | | | |
| 75 | System Security Plan (SSP) for 1099 Tax Reporting Program (1099TRP) | August 26, 2015 | | X | | |
| 76 | Incident Response Reporting Plan (IRRP), Defense Joint Military-Pay System (DJMS) | August 17, 2015 | | | X | |
| 77 | System Access Control Policy for Integrated Accounts Payable System (IAPS) | August 2015 | X | | | |
| 78 | System Security Plan (SSP) for International Civilian Pay System (ICPS) and Windows Automated Portuguese Pay System (WinAPPS) | August 2015 | | X | | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 79 | Incident Response Plan (IRP), Defense Retired and Annuity Pay System (DRAS) | July 24, 2015 | | | X | |
| 80 | System Security Plan (SSP) for Work Year Personnel Cost (WYPC) System | July 23, 2015 | X | | | |
| 81 | Information Assurance (IA) Access Control Policy, Defense Joint Military Pay System (DJMS) | June 26, 2015 | X | | | |
| 82 | Access Control Procedures, Transportation Support System (TSS) | June 22, 2015 | X | | | |
| 83 | DFAS Security Control Baseline Business Continuity Planning System | June 16, 2015 | X | | X | |
| 84 | ~~(FOUO)~~ [redacted] | June 15, 2015 | X | | | |
| 85 | ~~(FOUO)~~ [redacted] | June 2015 | X | X | X | |
| 86 | ~~(FOUO)~~ [redacted] | June 2015 | X | X | | |
| 87 | Business Continuity Planning System (BCPS) System Access Controls | June 2015 | X | | X | |
| 88 | System Access Control Policy, and Standard Operating Procedures for Online Report Viewing (OLRV) | May 12, 2015 | X | | | |
| 89 | System Security Plan (SSP) for Garnishment Electronic Document Management (EDM) System | May 4, 2015 | X | | | |
| 90 | System Security Plan (SSP) for Enterprise Portal (ePortal) | April 15, 2015 | X | X | X | |
| 91 | DFAS Security Control Baseline, Standard Accounting and Reporting System | March 25, 2015 | X | | | |
| 92 | Access Control Plan for the myPay System | March 20, 2015 | X | | | |
| 93 | 1099TRP, Configuration Management Plan (CMP) | February 26, 2015 | | X | | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 94 | Incident Response Plan (IRP), Operational Data Store (ODS) | January 21, 2015 | | | X | |
| 95 | Reviewing the Auditing Log Procedure for General Accounting and Finance System-Reengineered (GAFS-R) Oracle | January 15, 2015 | | | X | |
| 96 | DFAS Security Control Baseline, Case Management System | January 3, 2015 | X | | | |
| 97 | Access Control Policy (ACP) for Defense Disbursing Analysis Reporting System (DDARS) | January 2015 | X | | | |
| 98 | Incident Response Plan (IRP) Template | January 2015 | | | X | |
| 99 | System Security Plan (SSP) Template for Defense Business Management System | December 2014 | X | | X | |
| 100 | DFAS Acquisition Supplement (DAS), Part 52 - Solicitation Provisions and Contract Clauses, DAS 52.204-9001, DFAS Training Requirements | December 2014 | | | | X |
| 101 | System Security Plan (SSP) for Integrated Garnishment System | November 28, 2014 | X | X | X | |
| 102 | Service Level Agreement between Defense Information Systems Agency, Enterprise Information Services and Defense Finance and Accounting Service - Air Force | November 24, 2014 | | | | X |
| 103 | System Security Plan One Pay | November 17, 2014 | X | | X | |
| 104 | SSP: e-Authentication Plan, Garnishment Electronic Document Management (EDM) System (IGARN) | November 7, 2014 | X | | | |
| 105 | Reviewing the Auditing Log Procedure for General Accounting and Finance System-Reengineered (GAFS-R) UNISYS for DFAS I&T | November 6, 2014 | | | X | |
| 106 | ~~(U//FOUO)~~ [redacted] | November 2014 | | | X | |
| 107 | ~~(U)~~ Configuration Management Plan for Imaging Garnishment (IGARN) | October 20, 2014 | | X | X | ~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 108 | Reviewing the Auditing Log Procedure for Departmental Cash Management System (DCMS) Midtier Oracle | August 25, 2014 | X | | X | |
| 109 | Reviewing the Auditing Log Procedure for General Accounting and Finance System-Reengineered (GAFS-R) IBM for DFAS I&T | August 22, 2014 | | | X | |
| 110 | Audit Trail Procedures for CA-TSS | August 18, 2014 | | X | | |
| 111 | DFAS Security Control Baseline One Pay | August 13, 2014 | X | | | |
| 112 | Defense Working Capital Fund (DWCF) Service Level Agreement (SLA) between the Defense Information Systems Agency (DISA) Field Security Operations (FSO) and the Defense Finance and Accounting Service (DFAS) | July 8, 2014 | | | | X |
| 113 | ~~(FOUO)~~ [redacted] | June 17, 2014 | X | X | X | |
| 114 | System Security Plan (SSP) for Online Report Viewing (OLRV) | June 2, 2014 | X | | | |
| 115 | ~~(U//FOUO)~~ [redacted] | June 2014 | | | X | |
| 116 | DFAS Security Control Baseline, myPay Master PIN Data Base & myPay Web Administrator | May 10, 2014 | X | | | |
| 117 | DFAS Security Control Baseline, myPay - Web | May 10, 2014 | X | | | |
| 118 | Monitoring Security Violations Logs, Automated Disbursing System (ADS) | April 24, 2014 | | | X | |
| 119 | System Security Plan (SSP) for Defense Check Reconciliation Module (DCRM) | February 2014 | | X | | |
| 120 | Service Level Agreement between Defense Information Systems Agency, Enterprise Services Directorate and Defense Finance and Accounting Service (DFAS) | December 20, 2013 | | | | X |
| 121 | ~~(FOUO)~~ [redacted] | October 1, 2013 | | | | X<br>~~(FOUO)~~ |

Table 10 legend is located on the final table page.

*Table 10. Defense Finance and Accounting Service (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 122 | DFAS Memorandum of Understanding between Defense Joint Military Pay System-Active Component (DJMS-AC) and Case Management System (CMS) | September 6, 2013 | | | | X |
| 123 | DFAS Rome, Standard Operating Procedure (SOP), Standard Finance System (STANFINS) | June 20, 2013 | X | | | |
| 124 | ~~(FOUO)~~ [redacted] | June 14, 2013 | X | | | |
| 125 | System Access Controls | April 2013 | X | | | |
| 126 | Access Control Plan - Consolidated Returned Item Stop-Payment System (CRISPS) | March 28, 2013 | X | | | |
| 127 | System Security Plan (SSP) Template for Salary Offset Reporting System (SORS) | February 2013 | X | X | | |
| 128 | Security Access Procedures, Quarterly Review Procedure | October 23, 2012 | X | | | |
| 129 | Service Level Agreement between Defense Information Systems Agency, Enterprise Services Directorate and Defense Finance and Accounting Service (DFAS) - Accounting Services-Defense Agencies | August 15, 2012 | | | | X |
| 130 | Incident Response Plan (IRP) for Garnishment Imaging System (IGARN) | September 22, 2011 | | | X | |
| 131 | DFAS Memorandum: Blanket Consent to Monitor DFAS NIPRNet Command Communications Service Designator (CCSD) | September 21, 2010 | | | X | |
| 132 | DFAS 8400.1-R, Infrastructure | August 2008 | X | X | X | X |
| 133 | DFAS 8500.1-R, Information Assurance | November 2007 | X | X | X | X |
| 134 | Service Level Agreement between Director, Technology Services Organization, and Director for Information and Technology, SLA No. T01018 | June 5, 2001 | | | | X ~~(FOUO)~~ |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 11. Defense Human Resources Activity*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | Defense Manpower Data Center, Information Assurance (IA), Site Security Policy | *April 26, 2016* | X | | | |
| 2 | ~~(FOUO~~ [redacted] | *April 26, 2016* | X | X | X | |
| 3 | Procedures for Computer/Electronic Accommodations Program | *April 20, 2016* | | | X | |
| 4 | Defense Travel Management Office Procedures for Logical Access, Monitoring and Detecting, and Third-Party Service Providers | *April 20, 2016* | X | | X | X |
| 5 | Procedures for Employer Support of the Guard (ESGR) and Reserve Portal Information Security Management | *April 20, 2016* | X | X | X | X |
| 6 | ~~(FOUO~~ [redacted] | *April 19, 2016* | X | X | X | X |
| 7 | ~~(FOUO~~ [redacted] | *April 19, 2016* | X | | X | |
| 8 | Defense Civilian Personnel Data System (DCPDS), Software and License Inventory Procedures | *April 19, 2016* | | X | | |
| 9 | DoD OIG Requested Data for Defense Civilian Personnel Data System (DCPDS) | *April 19, 2016* | X | | X | |
| 10 | Defense Civilian Personnel Data System, Logical Access Process | *April 19, 2016* | X | | | |
| 11 | Procedures for the National Security Education Program Information Technology System (NSEP-IT) | *April 19, 2016* | X | | | X |
| 12 | Defense Civilian Personnel Data System, Security Management Plan | January 28, 2016 | X | | | |
| 13 | Computer/Electronic Accommodations Program, Administrative and Operating Procedures: Information Technology | November 23, 2015 | X | | X | |
| 14 | Performance Work Statement, Synchronized Pre-Deployment and Operational Tracker Enterprise Suite (SPOT-ES) | October 1, 2015 | | | | X |
| 15 | Defense Travel Management Office, Information Security, Configuration Management Policy | June 2, 2015 | | X | | ~~(FOUO)~~ |

Table 11 legend is located on the final table page.

*Table 11. Defense Human Resources Activity (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 16 | Defense Travel Management Office Passport Information Security Configuration Management Procedures | June 2, 2015 | | X | | |
| 17 | Defense Travel Management Office, Information Security, Access Control Policy | May 20, 2015 | X | | | |
| 18 | Defense Travel Management Office Passport Information Security, Access Control Procedures | May 20, 2015 | X | | | |
| 19 | Defense Personnel Records Information Retrieval System, System Security Plan | May 11, 2015 | X | | X | |
| 20 | ~~(FOUO)~~ [redacted] | February 9, 2015 | X | | X | |
| 21 | ~~(FOUO)~~ [redacted] | December 5, 2014 | | X | X | X |
| 22 | ~~(FOUO)~~ [redacted] | September 10, 2014 | X | | X | |
| 23 | ~~(FOUO)~~ [redacted] | March 24, 2014 | X | | X | |
| 24 | ~~(FOUO)~~ [redacted] | March 24, 2014 | X | | X | |
| 25 | ~~(FOUO)~~ [redacted] | March 21, 2014 | X | | X | |
| 26 | ~~(FOUO)~~ [redacted] | March 6, 2014 | X | | X | |
| 27 | ~~(FOUO)~~ [redacted] | January 10, 2014 | X | | X | |
| 28 | ~~(FOUO)~~ [redacted] | March 30, 2012 | X | X | X | |
| 29 | ~~(FOUO)~~ [redacted] | March 1, 2012 | X | | X | |
| 30 | ~~(FOUO)~~ [redacted] | September 10, 2010 | X | | X | ~~(FOUO)~~ |

Table 11 legend is located on the final table page.

*Table 11. Defense Human Resources Activity (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 31 | ~~(FOUO)~~ [redacted] | August 24, 2010 | X | | X | |
| 32 | ~~(FOUO)~~ [redacted] | September 23, 2009 | | | X | |
| 33 | ~~(FOUO)~~ [redacted] | February 12, 2008 | | | X | ~~(FOUO)~~ |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 12. Defense Health Agency*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | ~~(U//FOUO~~ [redacted] | March 22, 2016 | | | X | X |
| 2 | Network Operations Center - Host Security Services (HSS), Concept of Operations (CONOPS) | March 22, 2016 | | X | X | |
| 3 | ~~(U//FOUO)~~ [redacted] | March 22, 2016 | | | X | X |
| 4 | ~~(U//FOUO)~~ [redacted] | March 22, 2016 | | | X | X |
| 5 | ~~(U//FOUO)~~ [redacted] | March 22, 2016 | | | X | X |
| 6 | ~~(FOUO)~~ [redacted] | March 2016 | | | X | ~~(FOUO)~~ |

Table 12 legend is located on the final table page.

*Table 12. Defense Health Agency (cont'd)*

| ~~(FOUO)~~ Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 7 | ~~(FOUO)~~ [redacted] | March 2016 | | | X | |
| 8 | ~~(FOUO)~~ [redacted] | March 2016 | X | | | |
| 9 | ~~(FOUO)~~ [redacted] | March 2016 | | | X | |
| 10 | ~~(FOUO)~~ [redacted] | March 2016 | | | X | |
| 11 | ~~(FOUO)~~ [redacted] | March 2016 | X | | | |
| 12 | Network Security Operations Branch, Connection Approval Process, Standard Operating Procedures | March 2016 | | | | X |
| 13 | ~~(FOUO)~~ [redacted] | September 2015 | | | X | |
| 14 | ~~(FOUO)~~ [redacted] | September 2015 | | | X | |
| 15 | ~~(FOUO)~~ [redacted] | September 2015 | | | X | |
| 16 | ~~(FOUO)~~ [redacted] | September 2015 | X | | X | |
| 17 | ~~(FOUO)~~ [redacted] | September 2015 | X | | | |
| 18 | ~~(FOUO)~~ [redacted] | August 2015 | | | X | |
| 19 | ~~(FOUO)~~ [redacted] | August 2015 | | | X | |
| 20 | ~~(FOUO)~~ [redacted] | August 2015 | | | X | |
| 21 | ~~(FOUO)~~ [redacted] | August 2015 | | | X | |
| 22 | ~~(FOUO)~~ [redacted] | August 2015 | X | | X | |
| 23 | ~~(FOUO)~~ [redacted] | August 2015 | X | | | ~~(FOUO)~~ |

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

*Table 13. Missile Defense Agency*

| Number | Document Name | Date | L | S | MD | T |
|---|---|---|---|---|---|---|
| 1 | Information System Privileged Account Access Agreement and Acknowledgement of Responsibilities | *April 22, 2016* | X | | | |
| 2 | MDA Procedures - Action Item Matrix | March 9, 2016 | X | X | | X |
| 3 | MDA Manual 4161.01-M, MDA Property Accountability and Reporting | July 24, 2014 | | X | | |
| 4 | Policy Memorandum No. 69, Securing Ballistic Missile Defense Information on Government and Government Sponsored Networks and Systems | March 17, 2014 | X | | | X |
| 5 | Policy Memorandum No. 68, Securing Ballistic Missile Defense Information on Non-Government Sponsored Contractor Networks and Systems | April 10, 2013 | | | | X |
| 6 | MDA Plan 8500.02-P, Information Assurance Program Plan | October 3, 2007 | X | | | X |

Note: Dates in italics refer to the date we received the document from the Component because the document itself was not dated.

**LEGEND**

L Logical Access
S Software and License Inventory
MD Monitoring and Detecting Threats
T Third-Party Service Providers

# Appendix D

## Reports on Noncompliance with Logical Access Policies and Procedures

During the last 3 years, the DoD IG, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency issued seven reports that discussed logical access policies and procedures. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/pubs/index.cfm. Unrestricted Army Audit Agency reports can be accessed at https://www.aaa.army.mil. A list of Naval Audit Service reports can be accessed at http://www.secnav.navy.mil by selecting Audit Report Listings. Unrestricted Air Force Audit Agency reports can be accessed at https://www.efoia.af.mil/palMain.aspx by selecting the Freedom of Information Act Library and then selecting audit reports.

### *DoD IG*

DODIG-2014-037, "Systemic Physical and Cyber Security Weaknesses Within the U.S. Army Corps of Engineers," February 10, 2014

DODIG-2013-036, "Improvements Are Needed to Strengthen the Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division," January 14, 2013

### *Army Audit Agency*

A-2016-0088-IET, "Followup Audit of Elevated Privileges," May 3, 2016

A-2013-0137-FMT, "Elevated Privileges," August 20, 2013

### *Naval Audit Service*

N2015-0026, "Management Controls of Navy Corporate Data," July 16, 2015

N2013-0024, "Internal Controls Over Navy's Electronic Leave System," April 26, 2013

### *Air Force Audit Agency*

F2013-0016-O40000, Memorandum Audit Report of Reserve Travel System – Phase 1, General and Selected Application Controls, September 5, 2013

# Glossary

**Application.** A software program hosted on an information system.

**Authenticate.** To confirm the identity of an entity.

**Asset.** A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

**Commercial Off-the-Shelf.** A hardware or software product that is commercially made and available for sale, lease, or license to the general public.

**Covered Agency.** An agency that operates a covered system.

**Covered System.** A national security system, or a Federal computer system that provides access to personally identifiable information.

**Cryptography.** The discipline that embodies the principles, means, and methods for providing information security, including confidentiality, data integrity, nonrepudiation, and authenticity.

**Denial of Service.** Preventing authorized access to resources or delaying time-critical operations.

**Digital Rights Management.** Digital rights management is used to prevent unauthorized redistribution of digital media and restrict how information can be copied.

**Exfiltration.** An unauthorized transfer of information from an information system.

**Firewall.** A gateway that limits access between networks in accordance with local security policy.

**Forensics.** The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

**Government Off-the-Shelf.** A hardware or software product that is developed by the technical staff of a Government organization for use by the U.S. Government.

**Hardware.** The physical components of an information system.

**Host.** Any hardware device that has the capability of permitting access to a network. Examples include, but are not limited to, computer and personal electronic devices.

**Host-Based Security.** A set of capabilities that provide a framework to implement a wide range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that, together, provide automated protection to detect, respond, and report host-based vulnerabilities and incidents.

**Information System.** A discrete set of information resources organized to collect, process, maintain, use, share, disseminate, or dispose of information.

**Information Technology.** Any equipment or interconnected system or subsystem of equipment that is used to acquire, store, manipulate, manage, move, control, display, switch, interchange, transmit, or receive data or information.

**Intrusion Detection System.** Software used to monitor events occurring in a computer system or network and analyze them for signs of possible incidents.

**Intrusion Prevention System.** Software that includes capabilities of an intrusion detection system as well as the ability to stop possible incidents.

**Information Resources.** Information and related resources, such as personnel, equipment, funds, and information technology.

**Logical Access.** A process of granting or denying specific requests to obtain and use information and related information processing services.

**Multifactor Authentication.** The use of not fewer than two authentication factors such as something that is known to the user, an access device that is provided to the user, or a unique biometric characteristic of the user.

**National Security System.** A telecommunications or information system operated by the Federal Government that involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or that is critical to the direct fulfillment of military or intelligence missions.

**Network Analysis Tools.** Network software that collects, examines, and interprets network communications to identify and respond to events that violate the security policy or posture of the resources attached to the network or the network infrastructure.

**Nonrepudiation.** Protection against an individual falsely denying having performed a particular action.

**Personally Identifiable Information.** Any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity (for example, name, social security number, date and place of birth) or that can be linked or is linkable to an individual (medical, educational, financial, and employment information).

**Privileged User.** A user who has access to system control, monitoring, or administrative functions.

**Public Key Infrastructure.** The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system.

**Removable Media.** Portable data storage media that can be added to or removed from a computing device.

**Software.** Computer programs (which are stored in and executed by computer hardware) and associated data (which is also stored in the hardware) that may be dynamically written or modified during execution.

# Acronyms and Abbreviations

| | |
|---|---|
| **CJCSI** | Chairman of the Joint Chiefs of Staff Instruction |
| **DFAS** | Defense Finance and Accounting Service |
| **DHA** | Defense Health Agency |
| **DISA** | Defense Information Systems Agency |
| **HBSS** | Host-Based Security System |
| **MDA** | Missile Defense Agency |
| **NIST** | National Institute of Standards and Technology |


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

## Whistleblower Protection
### U.S. Department of Defense

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

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

**Congressional Liaison**
congressional@dodig.mil; 703.604.8324

**Media Contact**
public.affairs@dodig.mil; 703.604.8324

**For Report Notifications**
www.dodig.mil/pubs/email_update.cfm

**Twitter**
www.twitter.com/DoD_IG

**DoD Hotline**
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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