Office of Inspector General

Audit Report

REPORT REQUIRED BY CYBERSECURITY ACT OF 2015 SECTION 406—FEDERAL COMPUTER SECURITY

The Department of Transportation

Report Number: FI-2016-089

Date Issued: August 11, 2016

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: **<u>INFORMATION</u>:** Report Required by Cybersecurity Act of 2015 Section 406—Federal Computer Security
Department of Transportation
Report Number FI-2016-089

Date: August 11, 2016

From: Louis C. King
Assistant Inspector General
for Financial and Information Technology Audits

Reply to Attn. of: JA-20

To: DOT Chief Information Officer
DOT Chief Privacy Officer
FAA Chief Information Officer

In December 2015, President Obama signed into law the Cybersecurity Act of 2015.[1] Section 406—Federal Computer Security—of the act requires that not later than 240 days after enactment (by August 14, 2016), inspectors general submit reports to Congress that contain information on systems covered by the act—national security systems[2] (NSS) and Federal computer systems that provide access to personally identifiable information (PII).

As required by the act, we conducted this audit to identify the Department of Transportation's (DOT) (1) access controls, and (2) other information security management practices to safeguard information stored in DOT's systems covered by the Cybersecurity Act of 2015.

We conducted our work in accordance with generally accepted Government auditing standards. To meet our objective, we assessed a sample of 73 of 162 non-contractor and contractor systems[3] covered by the act that contained PII,

[1] Public Law Number 114-113, Division N—Cybersecurity Act of 2015.

[2] An NSS is an information system whose operation involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment integral to a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (40 U.S.C. § 11103).

[3] Non-contractor systems are DOT owned and operated systems while contractor systems are those owned or operated by contractors on behalf of DOT.

including one NSS identified by the Department. The results of our statistical sample allowed us to project the extent of selected information security policies and practices among covered systems. We also reviewed and analyzed data pertaining to the Department's policies for access controls and information security management practices to safeguard information stored in DOT's systems covered by the act; reviewed OIG's reports on audits of related subject areas; and interviewed information security personnel in the Office of the Chief Information Officer (OCIO) and the Operating Administrations (OA). See exhibit A for further details on our scope and methodology. Because this report—as required by the Cybersecurity Act of 2015—is primarily for informational purposes for Congress, we are not making recommendations at this time.

BACKGROUND

Section 406—Federal Computer Security—of the act requires inspectors general to submit reports to Congress that contain certain information on their agencies' covered systems. Each inspector general must report on:

- The agency's logical access[4] policies and practices for covered systems and whether the policies and practices follow appropriate standards.
- A description and list of the agency's access controls and multifactor authentication[5] that govern privileged users'[6] access to covered systems.
- Whether the agency uses access controls or multifactor authentication for access to covered systems, and if not, a description of the reasons why.
- A description of the agency's information security management practices regarding covered systems including (1) the agency's policies and procedures for conducting inventories of the covered systems' software and the associated licenses; (2) the capabilities the agency uses to monitor for and detect data loss and other threats, data-loss prevention,[7] forensics,[8] visibility,[9] and digital rights management;[10] and (3) a description of how the agency uses these capabilities or the reasons why it does not do so.

[4] Under the act, logical access control refers to the granting and denial of requests to access and use system information and related services.

[5] Under the act, multi-factor authentication refers to the use of at least two factors to authenticate the identity of each user. These factors include (1) something known only to the user, such as a password or personal identification number; (2) an access device provided to the user, such as a token; and (3) a unique biometric characteristic of the user.

[6] Under NIST SP 800-53, a privileged user is one that is authorized and therefore trusted to perform security-related functions that other users are not authorized to perform.

[7] A data-loss prevention capability monitors PII to prevent its unauthorized or inadvertent disclosure.

[8] Digital forensics analyze computer systems to determine the nature of possible security breaches and whether data have been accessed or lost.

[9] Visibility capabilities identify PII and monitor its movement.

[10] A digital rights management capability prevents unauthorized review, redistribution, and modification of sensitive information through data encryption, termination of access, and control of user access to data and actions, such as printing, that users can take.

- Finally, a description of the policies and procedures that ensure that entities, including contractors, that provide services to the Agency implement its information security management practices.

We addressed some of the act's requirements in our 2015 audit required by the Federal Information Security Management Act of 2002 (FISMA). During that audit,[11] we found that DOT had not completed implementation of multifactor user identity authentication using personal identity verification (PIV) cards for access to covered systems. We made a recommendation to strengthen DOT's requirements for the use of PIV cards.

RESULTS IN BRIEF

DOT has policies and practices[12] for logical access and multifactor user identity authentication for most systems. Additionally, the Department has procedures for multifactor authentication of privileged users' identities, but has not implemented them for many covered systems. Lastly, the Department does not have policies and practices for logical access to its NSS and does not use multifactor authentication for this system. See table 1 for a summary of the number of compliant systems in our sample. According to OCIO officials, the Department has not completed its implementation of multifactor user identity authentication in part due to unclear guidance and a lack of resources.

Table 1. Sample Systems Compliant with Access Control Requirements as of June 7, 2016

Requirement	Compliant non-contractor (DOT) systems		Compliant contractor systems*		Compliant national security systems (NSS)		Total number of compliant systems	
	Compliant	Reviewed	Compliant	Reviewed	Compliant	Reviewed	Compliant	Reviewed
Logical access policies & practices	42	42	30	30	0	1	72	73
Multifactor authentication required for privileged users	8	42	3	30	0	1	11	73

*In our FISMA audits for fiscal years 2014 and 2015, we found that some contractor systems were not categorized according to DOT policy. Specifically, five contractors systems that were identified in those two FISMA audits as not categorized according to DOT security policy are included in our sample as contractor systems.

Source: OIG analysis

[11] *DOT Has Had Major Success on PIV Implementation but Problems Persist in Other Cybersecurity Areas*, OIG Report Number FI-2016-001, November 5, 2015.

[12] DOT Cyber Security Compendium, June 2015.

DOT does not have adequate safeguards for much of the information stored in its covered systems because it has either not established or not implemented the following requirements or best practices: (1) policies and procedures for conducting inventories of software and associated licenses; (2) capabilities for data-loss prevention; (3) forensics and visibility capabilities sufficient to identify PII and monitor its movements; and (4) digital rights management capabilities. For example, only 1 of the 73 systems in our sample had software inventory policy and procedures. Also, the Department has acquired digital rights capabilities, but has not implemented them for any of the sampled systems. See table 2 for a summary of compliant systems in our sample. OCIO officials informed us that the Department has not implemented these capabilities due to a lack of funding.

Table 2. Sample Systems Compliant with Information Security Management Requirements or Best Practices as of June 7, 2016

Requirement (R) or best practice (BP)	Compliant non-contractor (DOT) systems		Compliant contractor systems***		Compliant national security systems (NSS)		Total number of compliant systems	
	Compliant	Reviewed	Compliant	Reviewed	Compliant	Reviewed	Compliant	Reviewed
Software inventory policies & procedures (R)	0	42	1	30	0	1	1	73
Data loss prevention practices (R)	34	42	4	30	0	1	38	73
Forensics & visibility practices (R)	0*	42	0**	30	0	1	0	73
Digital rights management practices (BP)	0	42	0	30	0	1	0	73

*All 42 non-contractor systems in our sample have forensics capabilities, but none has the visibility capabilities required by the act.

**Twenty-eight of 30 contractor systems in our sample have forensics capabilities, but none has the visibility capabilities required by the act.

***In our fiscal years 2014 and 2015 FISMA audits, we found that some contractor systems were not categorized according to DOT policy. Specifically, five contractors systems that were identified in those two FISMA audits as not categorized according to DOT security policy are included in our sample as contractor systems.

Source: OIG analysis

DOT HAS POLICIES AND PRACTICES FOR ACCESS AND AUTHENTICATION FOR MOST SYSTEMS, BUT IMPLEMENTATION IS INCOMPLETE

As required by the Cybersecurity Act, DOT has established policies and practices for logical access and multifactor authentication of users' identities for all covered systems except the NSS. However, the Department has not implemented multifactor authentication of privileged users' identities for many covered systems.

DOT Has Established Policies and Practices for Logical Access for Most Systems

DOT's Cybersecurity Compendium includes policy, guidance, and practices for logical access to systems that contain PII. The Department has established these policies for all covered systems except its NSS. Based on this finding, we estimate that 99.4 percent[13] of DOT's covered systems have logical access policies and practices.

DOT Has Not Implemented Multifactor Authentication for Privileged Users' Access to Many Covered Systems

The Cybersecurity Compendium requires that every departmental information system have capabilities for multifactor authentication of user identities for access to privileged accounts. However, in our FISMA 2015 audit, we found that the Department had not completed implementation of multifactor authentication for privileged users' identities. As of May 23, 2016, it had transitioned only 39 of DOT's 460 systems, including 11 of our 73 sample systems, to multifactor user identity authentication. Based on our findings, we estimate that only 16 percent[14] of DOT's covered systems use multifactor authentication of users' identities for access.

According to OCIO officials, the Department has not implemented multifactor user identity authentication for all covered systems for four reasons. First, the Department's guidance does not provide clear direction on how to enable systems for use of PIV cards—one important factor for multifactor identity authentication. Second, the Department's guidance has contributed to confusion for OAs regarding reporting on use of PIV cards as a factor for identity authentication and consequently underreporting of PIV-enabled systems. Third, departmental resources for oversight of the transition to PIV card use by the Office of the Chief Information Security Officer (CISO) have been significantly limited. In 2012, the position allocated to oversee the transition was reclassified for incident response duties, and resources to hire for the position were not available until fiscal year 2016. Consequently, since that time the CISO has been performing oversight functions with the assistance of a small contract staff. Finally, the OAs' fixed or declining budgets have constrained investment in this and other cybersecurity priorities.

[13] Our 99.4 percent estimate has a 90-percent lower confidence limit of 96.2 percent.
[14] Our 16.0 percent estimate has a precision of +/-5.7 percentage points at the 90-percent confidence level.

THE DEPARTMENT DOES NOT HAVE ADEQUATE SAFEGUARDS FOR MUCH OF THE INFORMATION STORED IN ITS COVERED SYSTEMS

DOT has either not established or implemented the appropriate actions to safeguard the information on its systems covered by the act. Specifically, the Department has not established or not implemented: (1) policies and procedures for conducting inventories of software and associated licenses; (2) capabilities for data-loss prevention; (3) forensics and visibility capabilities sufficient to identify PII and monitor its movements; and (4) digital rights management capabilities.

The Department Has Not Implemented Policies and Procedures for Conducting Inventories of Software and Licenses for the Majority of Covered Systems

DOT has not implemented policies and procedures for conducting inventories of software on most covered systems and the associated licenses. According to National Institute of Standards and Technology (NIST) guidelines,[15] to manage software asset and licensing information, agencies should track license compliance, monitor usage, and manage software assets' life cycles. We found that the Department had implemented these policies and procedures for only 1 of our 73 sample systems. Based on this finding, we estimate that 1.1 percent[16] of DOT's covered systems had policies and procedures for conducting inventories of software and associated licenses.

The Department Has Not Implemented Data Loss Prevention Capabilities for Most Covered Systems

DOT has a data loss prevention capability in place for only some covered systems. NIST guidelines[17] recommend that agencies monitor PII for unusual or suspicious events that may indicate data losses. We found that the Department had implemented its data loss prevention capability for 38 of our 73 sample systems. Based on this finding, we estimate that 58.7 percent[18] of DOT's covered systems had data-loss prevention capabilities. OCIO officials told us that the Department is in the process of procuring this capability for the rest of its covered systems.

[15] NIST Special Publication 800-137 (2010).

[16] Our 1.1 percent estimate has a 90-percent upper confidence limit of 2.2 percent.

[17] NIST Special Publication 800-122 (2010).

[18] Our 58.7 percent estimate has a precision of +/-5.8 percentage points at the 90-percent confidence level.

DOT Has Not Implemented Forensics Capabilities for All Covered Systems and Its Visibility Capability Cannot Detect Unauthorized PII Access and Loss

DOT has not implemented forensics capabilities—used to examine possible security breaches and determine whether data have been accessed or lost—for all covered systems. We found that the Department had not implemented forensics capabilities for 3 of our 73 sample systems. Furthermore, its visibility capability is inadequate because it cannot identify PII and monitor its movement within the Department. The monitoring that NIST's guidelines recommends provides agencies with sufficient visibility capabilities but the Department has not established this recommended monitoring for all its covered systems. An OCIO official informed us that in the future, the data loss prevention procurement will include a sufficient visibility capability for covered systems.

The Department Does Not Have Capabilities for Digital Rights Management for Covered Systems

DOT does not have digital rights management capabilities for all its covered systems. The Department has Microsoft Rights Management Services—designed to manage digital rights for data that flow through Microsoft products—but it had not implemented these capabilities for covered systems. Under OMB's guidance for non-national security systems,[19] Federal agencies should establish capabilities that secure their digital rights—rights to information in digital form—through the prevention of unauthorized review, redistribution, and modification of sensitive information. Best practices for digital rights management capabilities include: limits to user access to data; enforcement of rules and permissions for opening and reading, printing, modifying or editing, saving to clipboards, and other user actions; and persistent protection of data both internally and externally with expiration and revocation of data access and with encryption.

OCIO officials stated that the Department had not fully implemented the digital rights management capabilities department wide due to a lack of funding.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided the Department with a draft copy of this report on July 15, 2016, and received its response on August 4, 2016. DOT's response is included in its entirety in the appendix to this report. In its response, the Department emphasized its

[19] OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* (October 2015).

commitment to strengthening cybersecurity and protecting sensitive information, and national security systems.

ACTIONS REQUIRED

We made no recommendations in this report that require Agency actions at this time.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407, or Abdil Salah, Program Director, at (202) 366-8543.

#

cc: DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted this audit between March 2016 and July 2016. We conducted our audit work in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Generally accepted Government auditing standards also require us to disclose impairments of independence or any appearance thereof. Because OIG is a small component of the Department and has only 1 of the 73 systems in our sample, any assessment pertaining to OIG or its systems does not impair our ability to conduct this mandated audit.

Our objective was to identify the DOT (1) access controls, and (2) other information security management practices to safeguard information stored in DOT's systems covered by the Cybersecurity Act of 2015. This audit will also support our Federal Information Security Modernization Act audit.

OIG's Statistician selected a stratified random attribute sample of 73 out of 162 non-contractor and contractor systems covered by the act that contained PII, including 1 of 1 non-contractor NSS identified by the Department. Our sample design allowed us to estimate compliance with several different requirements with 90-percent confidence and a precision no greater than 5.8 percentage points. To meet our objective, we reviewed previously issued OIG reports related to our audit; interviewed personnel in the Office of the Chief Information Officer and OA information system security managers and system owners; and reviewed and analyzed the Department's policies for access controls and information security management practices to safeguard information stored in DOT's covered systems.

To ensure accuracy and completeness of DOT's covered systems and associated documentation, we validated the Department's inventory against data collected during FISMA and other classified audits, and we sampled 73 systems. Based on our review we deemed the Department's PII system inventory sufficiently reliable for the purposes of our audit.

EXHIBIT B. ENTITIES VISITED OR CONTACTED

Department of Transportation Headquarters

- Federal Highway Administration (FHWA)
- Federal Railway Administration (FRA)
- Federal Motor Carrier Safety Administrator (FMCSA)
- Federal Transit Administration (FTA)
- Maritime Administration (MARAD)
- National Highway Traffic Safety Administration (NHTSA)
- Office of Inspector General (OIG)
- Office of the Secretary (OST)
- Volpe National Transportation Systems Center (Volpe)
- Office of the Chief Information Officer (OCIO)

Federal Aviation Administration Headquarters

- Federal Aviation Administration (FAA)

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Abdil Salah	Program Director
Severin Pefoubou	Project Manager
Lissette Mercado	Information Technology Audits Advisor
James Mullen	Information Technology Specialist
Justin Ubert	Information Technology Specialist
Zachary Lewkowicz	Information Technology Specialist
Shavon Moore	Information Technology Specialist
Petra Swartzlander	Senior Statistician
Makesi Ormond	Statistician
Susan Neill	Writer-Editor
Amy Berks	Senior Counsel

APPENDIX. AGENCY COMMENTS

U.S. Department of
Transportation
Office of the Secretary
of Transportation

MEMORANDUM

Subject: **INFORMATION**: Management Response – Office of Inspector General (OIG) Report on the Cybersecurity Act of 2015

Date: August 3, 2016

From: Richard McKinney
DOT Chief Information Officer

RICHARD MCKINNEY
Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=RICHARD MCKINNEY
Date: 2016.08.03 15:25:59 -04'00'

Reply to attn. of:

To: Louis C. King
Assistant Inspector General for
Financial and Information Technology Audits

The U.S. Department of Transportation (DOT) takes seriously its responsibilities to protect sensitive information, and national security systems. DOT has invested in enterprise services, and capabilities that system owners can cost-effectively leverage for improved security, while ensuring improved visibility into security weaknesses, and reduced times for the remediation of critical vulnerabilities. Examples of investments and engagements that are reflective of our efforts include:

- Collaborating with the National Security and Intelligence communities to enforce existing policies and employ shared services such as the Homeland Secure Data Network (HSDN), the Joint Worldwide Intelligence Communications System (JWICS), and the National Security Service Public Key Infrastructure Common Service Providers (NSS PKI CSP).
- Developing enterprise authentication and authorization services to enable the use of Personal Identity Verification (PIV) smart cards for secure access to agency computer systems.

- Deployment of digital rights management and data loss prevention tools to protect sensitive information, and to detect unauthorized transmission of data outside of the agency.

The Department is committed to strengthening cybersecurity while preserving mission and business availability. We will continue to exercise due diligence in our oversight and enterprise governance to identify opportunities to reduce risks across the agency, and seek solutions and partnerships that achieve improvements in the Department's cybersecurity posture.

We appreciate the opportunity to respond to the OIG draft report. Please contact Andrew Orndorff, Associate CIO / Chief Information Security Officer (CISO), at (202) 366-7111 with any questions or if you would like to obtain additional details.