Office of Inspector General
Audit Report

FISMA 2015: DOT HAS MAJOR SUCCESS IN PIV IMPLEMENTATION, BUT PROBLEMS PERSIST IN OTHER CYBERSECURITY AREAS

Department of Transportation

Report Number: FI-2016-001
Date Issued: November 05, 2015

~~**FOR OFFICIAL USE ONLY. Public Availability To Be Determined under 5 U.S.C. § 552, Freedom of Information Act.**~~

Memorandum

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

Subject: **ACTION:** FISMA 2015: DOT Has Major Success in PIV Implementation, But Problems Persist In Other Cybersecurity Areas Department of Transportation Report Number: FI-2016-001

Date: November 05, 2015

From: Calvin L. Scovel III
Inspector General

Reply to Attn. of: JA-20

To: Deputy Secretary

(~~FOUO~~) The Department of Transportation's (DOT) operations rely on 463 information technology (IT) systems, nearly two-thirds of which belong to the Federal Aviation Administration (FAA). The Department considers more than [redacted] of these systems as high-value assets[1] with data that are of potential interest to hackers. These systems represent an annual investment of approximately $3 billion—one of the largest IT investments among Federal civilian agencies. Moreover, the Department's financial IT systems are used to award, disburse, and manage approximately $117 billion in Federal funds annually.

Maintaining an effective information security program—one that quickly identifies and addresses vulnerabilities—is critical to ensuring continuity of operations and thwarting individuals who attempt to gain unauthorized access to systems and information. For DOT, securing information not only protects taxpayers' dollars but their safety as well, since many DOT IT systems control transportation-related operations, including air traffic management, and pilot

[1] In 2015, the Office of Management and Budget (OMB) launched the Federal Cyber Sprint initiative that directs agencies to further protect Federal information, improve network resilience, and report to OMB on their successes and challenges and on what systems they consider high-value assets. Assets, systems, and datasets are determined to be high-value based on the following attributes: sensitivity of the information, uniqueness of the dataset, impact of loss or compromise, system dependencies, and systems that are integral to supporting critical departmental communications.

licensing and fitness, or support agency inspection and oversight for highway safety, and hazmat transport.

The Federal Information Security Management Act of 2002 (FISMA), as amended,[2] requires agencies to develop, implement, and document departmentwide information security programs. FISMA also requires program officials, chief information officers (CIO), and inspectors general to conduct annual reviews of their agencies' information security programs, and report the results of these reviews to the Office of Management and Budget (OMB). As part of this review, OMB requires Inspectors General to use 87 metrics in 10 security areas[3] to assess the effectiveness of their agencies' programs.

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices for the 12-month period between July 1, 2014, and June 30, 2015.[4] Specifically, we assessed DOT's (1) information security policy and procedures, (2) enterprise-level information security controls,[5] (3) system-level security controls, and (4) management of information security weaknesses.

We conducted our work in accordance with generally accepted Government auditing standards. To address OMB's 2015 FISMA reporting metrics, we assessed 24 sample systems and analyzed data in the Department's Cybersecurity Assessment and Management system (CSAM), a repository for tracking system inventories, weaknesses, and other security information. We also tested software settings in six general support systems, reviewed supporting documentation, and interviewed Department officials. As part of this work, we selected a statistical sample of 762 computers out of 83,621 that allowed us to project that 85 percent[6] of DOT's computers are compliant with federally prescribed configuration

[2] The Federal Information Security Modernization Act of 2014 amends FISMA to, among other things,(1) reestablish the oversight authority of the Director of OMB with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.
[3] OMB's security areas include risk management, contingency planning, and identity and access management, among others.
[4] Per OMB's Annual Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, agencies should set cut-off dates for data collection and report preparation that allow adequate time for meaningful internal reviews, comments, and resolution of disputes before reports' finalization.
[5] For purposes of this report, enterprise-level controls are not system-specific and include information security continuous monitoring, security training, incident response and reporting, account and identity management, and configuration management.
[6] Our estimate has a margin of error of +/-8.6 percentage points at the 90 percent confidence level.

standards.[7] See exhibit A for more details on our scope and methodology. As required, we provided our results to OMB via its Web portal.[8]

RESULTS IN BRIEF

Since our 2014 review, the Department has made major progress in implementing the required use of PIV cards for all DOT employees and contractors.[9] DOT reported issuing PIV cards to 100 percent of its employees, and 98.3 percent have been configured for use in accessing networks, which represents an increase of 74.5 percent from last year. However, the Department's information systems remain vulnerable to serious security threats due to the following deficiencies.

1. In response to our prior recommendations, the Office of the Chief Information Officer (OCIO) issued its information security policy. However, gaps remain in key areas such as risk management and continuous monitoring. OCIO's policy required Operating Administrations (OA)[10] to develop compliant procedures within one year. The OAs are still missing procedures in key areas such as control testing. These gaps in DOT policies and procedures have contributed to the security weaknesses we identified in this and prior FISMA reports.

2. DOT's enterprise-level controls—controls that must be implemented across the Department—remain inadequate despite successes in PIV implementation. For example, DOT has not completed implementation of system log-in and facility access by PIV cards as required. In addition: (a) DOT's information security continuous monitoring (ISCM) program lacks sufficient maturity to be effective; (b) OAs do not disable user accounts after 90 days of inactivity in accordance with DOT policies, and DOT does not consistently perform

[7] United States Government Configuration Baselines (USGCB) are security configuration settings developed by the National Institute of Standards and Technology (NIST), the Department of Defense, and DHS for certain Windows operating systems.
[8] Because OMB designates this information "For Official Use Only," our submission to OMB is not contained in this report.
[9] A PIV card is a smart card that contains the necessary data for the holder to be granted access to Federal facilities and information systems and assure appropriate levels of security for all applicable applications.
[10] DOT has 12 components: FAA, the Federal Highway Administration (FHWA), the Federal Motor Carrier Safety Administration (FMCSA), the Federal Railroad Administration (FRA), the Federal Transit Administration (FTA), the Maritime Administration (MARAD), the National Highway Traffic Safety Administration (NHTSA), the Pipeline and Hazardous Materials Safety Administration (PHMSA), the Saint Lawrence Development Seaway Corporation (SLDSC), the Office of the Secretary of Transportation (OST), the Office of the Inspector General (OIG), and the Surface Transportation Board (STB). In prior years, the Research and Information Technology Administration (RITA) was considered a separate component, but is now part of OST. For purposes of this report, the 12 components are referred to as Operating Administrations.

periodic reviews of information system accounts that are not assigned to specific users;[11] (c) DOT's Cyber Security Management Center (CSMC)[12] does not yet have direct visibility of FAA operational networks, and FAA did not report all required security incidents to CSMC or the United States Computer Emergency Readiness Team (US-CERT);[13] (d) some departmental computers do not meet required security standards for use of commercial software; (e) DOT does not have a mature risk management program;[14] and (f) DOT has not fully implemented a method for tracking contractors' completion of security training;

3. DOT's controls remain insufficient to protect system security. Five OAs have not implemented NIST's risk management framework,[15] per departmental policy, to identify and manage system risks. In addition, (1) six OAs have allowed systems' authorizations-to-operate to expire; (2) OCIO and OAs have not established effective procedures for common security controls; (3) eight OAs do not properly test controls between system authorizations; and (4) six OAs have not maintained up-to-date contingency plans for use in the event of an emergency system shutdown. FAA also has not established an accurate inventory of its contractor operated systems, and six OAs using cloud computing services did not satisfy OMB's cloud requirements.

4. DOT does not sufficiently oversee the remediation or closure of plans of action and milestones (POA&M). OAs did not include all security weaknesses in CSAM. For example, FAA did not document control weaknesses in CSAM for over 150 audit recommendations to address significant security weaknesses in its air traffic control information security program that Government Accountability Office (GAO) reported in 2015. For 2,023 of the 3,820 open POA&Ms that OAs did report to CSAM, OAs did not have actual start dates for weakness remediation. For 960 POA&Ms, OAs did not identify the cost to remediate the weaknesses.

We are making a series of recommendations to assist the Department in establishing and maintaining an effective information security program—one that

[11] Information system accounts include shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service accounts.
[12] CSMC analyzes incident reports, categorizes each incident by type, and reports all incidents to US-CERT.
[13] US-CERT, managed by DHS, collects reports from Federal agencies on possible security breaches to information systems and provides information to reporters on corrective actions to take to resolve weaknesses.
[14] A risk management program manages and monitors risk at three levels: enterprise, business process, and system.
[15] The risk management framework is a structured process to assess risk during the system development life cycle. For example, the first step in the process is categorizing a system as high, medium, or low risk based on the impact of its loss to agency missions.

complies with FISMA, OMB, and other requirements. See table 15 in exhibit B for a summary of the recommendations from our six previous FISMA reports that remain open.

BACKGROUND

Under FISMA, each Federal agency must secure the information and information systems that support the agency's operations, including those provided or managed by other agencies, contractors, or other entities. Similarly, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires Federal agencies to ensure that appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. FISMA also requires each agency to report annually to OMB, Congress, and the GAO on the effectiveness of its information security policies, procedures, and practices.

DOT's 12 components (which we refer to as OAs in this report) manage the Department's 463 information systems. The Department relies on these systems to carry out its missions, including ensuring safe air traffic control operations, qualified commercial drivers, and safe vehicles. DOT must also ensure the integrity of data and reports that account for the billions of dollars used for many projects such as highway reconstruction and high-speed rail development.

For 2015, OMB required inspectors general to use 87 metrics in 10 security areas to assess their agencies' programs. Of these 10 areas, ISCM receives the greatest emphasis and updates to it metrics. ISCM entails the detection and prioritization of risks and allows an agency to prioritize resolution of and correct deficiencies. To establish a sound ISCM program, an agency must define staff roles and responsibilities, processes, and technology used to detect and correct risks and vulnerabilities. OMB, in its memorandum M-14-03,[16] requires agencies to implement ISCM in 3 phases. Phase 1 consists of an agency's transition from its legacy, point-in-time risk management program to a program that produces near real-time risk management. In real-time management, systems—including hardware, software, and configurations—are set to automatically detect and mitigate risk.

The Council of Inspectors General on Integrity and Efficiency (CIGIE)[17] introduced a new methodology for inspectors' general 2015 FISMA reporting. This methodology consists of a maturity model and is being deployed for the first time only in the area of ISCM. Both OMB and DHS required the use of this model, which helps inspectors general assess the maturity of ISCM within their

[16] OMB M-14-03, November 2013.
[17] CIGIE developed the model in coordination with OMB, NIST, and DHS.

agencies' on a scale of 1 to 5, with 1 representing the lowest level of maturity and 5 the highest. Table 1 identifies and defines each level.

Table 1. Maturity Model Levels and Definitions

Level	Definition
1—Ad Hoc	Agency still must define roles and responsibilities, processes, and technology.
2—Defined	Agency defined these but has not implemented them throughout the agency.
3—Consistently Implemented	Agency fully implemented its ISCM program but has not developed a metrics to measure the effectives of the program.
4—Managed and Measureable	Agency uses metrics to measure and manage the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.
5—Optimized	Agency's ISCM program is institutionalized and updated in near real-time based on changing in mission requirements, technology, and threats.

Source: U.S. Department of Homeland Security, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*, V1.2, June 19, 2015.

Since 2001, according to FISMA requirements, we have published 14 reports that present the results of our evaluations of the weaknesses in DOT's information security program and practices (see exhibit A).

SOME KEY INFORMATION SECURITY POLICIES ARE NOT COMPLETE

FISMA requires each department's CIO to develop and maintain information security policies and procedures to address security requirements. Agencies develop supporting guidance and procedures on how to effectively implement specific controls to augment security policy. DOT's OCIO may also delegate to the 12 OAs the authority to create procedures that comply with departmentwide policies. In response to our prior recommendations, OCIO issued its policy and required OAs to complete compliant procedures within 1 year. However, in three areas—continuous monitoring of controls, personal identity verification, and risk management—OCIO and OAs have not completed the required policies and procedures (see table 2).

Table 2. Deficiencies in DOT Information Security Policies and Procedures

Security Area Purpose and Requirements	Deficiency
Continuous Monitoring of Controls	
ISCM maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Processes that support ongoing security monitoring across the agency must include leadership's definition of a comprehensive ISCM strategy that encompasses people, processes, and technology.	OCIO's strategy lacks comprehensive guidance for implementation, monitoring, reporting, and enforcement for effective real-time cybersecurity monitoring.
Personal Identity Verification	
PIV is the governmentwide initiative to provide users of Federal networks with ID cards that use smart-card technologies to control access to Federal facilities and resources.	In 2014, OCIO implemented a waiver program for OAs that have unique problems or challenges in meeting Federal PIV requirements. This year, OCIO reported the waiver process has been retired and replaced with project plans but it has not updated its policy to reflect this change.
Risk Management	
For common controls—controls used by multiple systems—agencies must test controls, identify risks, determine whether they can accept the risks, and authorize the systems to operate.	OCIO and OAs have not finalized their procedures for control testing and risk assessment for common controls.
NIST 800-53, revision 4 covers implementation of security controls and requires agencies to assess new controls and enhancements.	DOT's policy and guidance do not address this revision 4. Furthermore, the policy allows OAs 2 years to implement testing of new security controls instead of 1 year as NIST security standards and guidelines call for.

Source: OIG analysis

This lack of policy and procedures for implementing security requirements or enforcement creates a risk that OAs will not properly apply security controls to their information systems. Furthermore, the deficiencies have contributed to the other security weaknesses we identified in this and prior FISMA reports.

DOT CONTINUES TO LACK ADEQUATE ENTERPRISE-LEVEL CONTROLS

DOT's enterprise-level controls—controls that must be implemented across the Department—remain inadequate, despite major progress in PIV deployment. Specifically, (1) DOT has not completed PIV access implementation; (2) DOT's ISCM program lacks sufficient maturity to be effective; (3) DOT lacks sufficient controls over user accounts and identity access management, and does not consistently perform periodic reviews of information system accounts that are not associated with a particular individual; (4) CSMC does not have direct visibility into FAA's operational networks, and FAA did not report all required security incidents to CSMC or US-CERT; (5) some departmental computers do not meet required security for use of commercial software; and (6) DOT's risk management program is not mature; and (7) DOT has not fully implemented its process to track contractors' completion of security awareness training completion.

DOT Reported Major Progress in PIV Implementation but FAA Data Are Questionable

OMB requires agencies to implement the full use of PIV credentials for access to Federal facilities and their information systems. OMB also required that, by 2012, all Federal personnel use PIV cards to log on to agency computers for multifactor user identity authentication.

DOT reported issuing PIV cards to 100 percent of its employees who have unprivileged accounts and a total of 98.3 percent have been configured for use in accessing networks. DOT also reported that 100 percent of its privileged accounts PIV cards are issued and configured for system use (see table 3). In addition, the Department has revoked the use of PIV card waivers, which were used for 27,851 unprivileged accounts last year.

Table 3: PIV Use for Unprivileged and Privileged Accounts

OA	Unprivileged Accounts			Privileged Accounts			
	Total	Yet To Be Provisioned	Percent Provisioned	Total	User Rights Reviewed	User Rights Adjusted	Percent Provisioned
FAA	46,355	0	100.0	172	172	0	100.0
FMCSA	1,340	0	100.0	28	28	1	100.0
FTA	727	2	99.7	27	27	3	100.0
NHTSA	1,033	6	99.4	24	24	3	100.0
OST	2,437	246	89.9	144	144	3	100.0
SLSDC	129	1	99.2	3	3	0	100.0
Total	**58,723**	**985**	**98.3**	**542**	**542**	**16**	**100.0**

Source: OCIO's report on departmental PIV access, July 14, 2015

These data indicate remarkable progress; however, we could not verify or support FAA data. We noted discrepancies between the data reported to us and to OCIO. For example, OCIO reported that FAA had issued 46,355 PIV cards, while FAA reported it had issued 44,614; further, the Federal Personnel System shows 45,423. Similarly, FAA reported provisioning 43,318 cards, while OCIO reported FAA issued 46,355 cards and met 100 percent provisioning.

In addition, the Department could only demonstrate slow progress on the number of applications that required the use of PIV cards for access. In 2014, 90 of 445 applications on DOT's network required access with PIV cards. In 2015, DOT only enabled 50 additional systems for PIV access. While FAA provided a plan that called for enabling its 318 applications by September 30, 2015, it subsequently reported that it converted only 143.

The use of PIV cards for physical access to DOT facilities has also been slow. According to OST, it has limited control over PIV implementation in leased facilities. FAA management reported that it plans to make all FAA facilities use PIV cards for access by the end of fiscal year 2018. The plan shows that 530 facilities currently do not use PIV for access (see table 4).

Table 4: FAA's Plan for Enabling Facilities to use PIV Cards

Fiscal Year	Facilities To Be PIV Enabled
2016	75
2017	205
2018	250
Total	**530**

Source: FAA

This lack of full use of PIV cards for access to the Department's information systems and facilities makes it difficult for DOT to ensure that system users and individuals that access facilities are correctly identified as authorized personnel.

DOT's ISCM Program Is at the Lowest Maturity Level

DOT's ISCM program is at a Level 1 maturity, leaving the Department's systems vulnerable to exploitable hardware and software. OAs use different tools for hardware and software management and to identify and resolve vulnerabilities. Their inventory systems are also not fully automated and are labor intensive to reconcile. Without an effective ISCM program, the agency's systems will be operating with numerous exploitable hardware and software vulnerabilities.

DOT's Hardware Asset Tracking Is Incomplete

The Department lacks a standardized process for tracking all IT hardware assets, and OCIO was not able to provide an accurate inventory of IT devices—servers, desktop computers, laptops, and notebooks—on DOT's networks. In its 2015 third-quarter report to OMB,[18] DOT reported a total of 123,077 hardware assets, including 85,614 IT devices. We tried to verify this number using four sources:

- The automated enterprise continuous monitoring system (AECM)—a tool nine OAs[19] use to monitor system security controls and create device inventories.
- The Active Directory which maintains information on most network resources, such as servers, work stations, and printers.
- OCIO asset reports.
- Individual OA report.

[18] Federal agencies must report to OMB on a quarterly basis regarding the security metrics that OMB has defined.
[19] FAA, STB, OIG, and the Volpe Center, which is part of OST, do not use it.

None of these sources agree with the total reported to OMB nor could they be reconciled to one another. In addition, none of the DOT tools could provide comprehensive lists of all network devices. Table 5 summarizes DOT's hardware inventory based on the available sources.

Table 5: Summary of Hardware Assets

Operating Administration	AECM System[a]	Active Directory Report for DOT Networks[b]	Inventory	
			OCIO[c]	OAs[d]
FAA		70,693	Not provided	50,780
FHWA			2,625	2,625
FMCSA			1,195	1,195
FRA			1,128	1,208
FTA			848	848
MARAD			773	773
US Merchant Marine Academy		2,794	Not provided	Not provided
NHTSA			1,328	3,780
OIG		701	Not provided	Not provided
OST			1,656	20
Common Operating Environment		15,658	11,098	
Volpe		1,863	Not provided	526
RITA			258	
PHMSA			803	803
SLSDC			84	Not provided
STB		291	Not provided	918
Totals	**24,598**	**92,000**	**21,796**	**63,476**

[a] Report of October 2014. Rather than by individual OAs, these data identify total devices per configuration checklist—USGCB, Defense Information Systems Agency Security Technical Implementation Guide, and Center for Internet Security baselines.
[b] Network scans of active computers.
[c] As of April 2015.
[d] As of July 2015.
Source: OIG analysis

DOT's Software Asset Inventory Is Also Incomplete

DOT also lacks a complete inventory of its software assets. For example, FAA's report contained a list of software applications but did not indicate which devices contained each application, and SLSDC only provided a list of software used for devices with Windows 7. Several weaknesses underlie DOT's inability to report complete inventory data to OMB per OMB requirements for Federal Departments:

- OCIO has not defined standards for the data OAs must report.
- While DOT requires monthly reporting on software asset management, some OAs only report annually.
- OAs' use different tools for collecting information on their software inventories.

DOT Has Not Fully Automated and Integrated Configuration Setting Management and Common Vulnerability Management

In addition to managing hardware and software assets, ISCM requires the development and implementation of two key concepts:

1. Configuration setting management (CSM): New software and hardware have default settings that can be changed. For example, the password length can be set to certain number or types of characters. CSM is the process where system administrators adjust these settings to Department standards. As requirements or standards change, the administrator will adjust the settings to match. Ideally, the administrator will automate the process to adjust settings.

2. Common vulnerability management (CVM): Throughout the life of software and hardware, users will discover security weaknesses. Software designers develop "patches" to remediate these weaknesses. It is up to users to apply these patches. Ideally, administrators will automate the process of applying patches as soon as a weakness is identified. If patches do not exist, administrators will monitor the status of the vulnerability and identify compensating controls.

However, DOT has not automated and integrated configuration setting management or common vulnerability management, and OAs provided no evidence that they have remediated security weaknesses for hundreds of computers. Among our sample systems, OAs have not properly implemented configuration settings or completed corrective actions for a number of deficiencies (see table 6).

(~~FOUO~~) Table 6: Configuration Setting and Common Vulnerability Deficiencies

System	Weaknesses Identified
Common Operating Environment [redacted]	• Evidence that identified vulnerabilities have been remediated was lacking. • A configuration baseline compliance scanning solution was not in place for network devices. • Configuration changes were not tested, validated, or documented.
FAA Aviation Safety (AVS) Air Transportation Oversight System [redacted]	• A process for assigning vulnerabilities to responsible entities, and tracking and reviewing those findings to completion was not in place. There is no evidence that AVS management is notified of these findings. • Scans for the presence of unauthorized software were not conducted on a regular basis.
OST Enterprise Support System [redacted]	• Vulnerabilities discovered during monthly scanning were not mitigated within the 90-day time frame specified in DOT policy. There is no evidence that POA&Ms are entered into CSAM within this time frame. Vulnerability testing for Web applications' known weaknesses was not performed. • Patches to commercial applications were not applied to correct system vulnerabilities in accordance with DOT Policy. • Evidence that OST reviews, approves, documents, and retains records of system changes in accordance with DOT policy was lacking. • Systems contain deviations from the approved baselines that have not been approved in accordance with DOT Policy.
FMCSA's LAN Segment at Volpe [redacted]	• Web application scans were not run on a regular basis, and the recommended frequency for conducting system vulnerability scans has not been defined. • Software updates for effectiveness were not tested before they were installed. • According to the last security assessment report, baseline scan results for this system indicate the servers are less than 30 percent compliant.
MARAD's Cargo Preference Overview System	• Evidence was not provided that vulnerability scans were conducted, reviewed, and addressed. • The recommended frequency of automated scans of configuration settings has not been defined. • Approvals of configuration changes were not documented with consideration for security impact analyses. • Baseline configurations were not document. • Security configuration checklists have not been defined.
FTA's Transportation Electronic Award Management System	• POA&Ms were not developed or timely risk assessment procedures were not performed within 30 days of detection of 2 high risk vulnerabilities on Windows servers as required by DOT policy. • A list of changes made to production files in fiscal year 2015 could not be produced. • Password configuration compliance could not be confirmed for the system's data repository.
[redacted]	

Source: OIG analysis

DOT's Controls for Account and Identity Management Are Deficient

DOT's account and identity management controls for the networks that service approximately 67,000 of the Department's accounts are deficient in several areas, including disabling accounts and periodic reviews of information system accounts. To minimize the risk that individuals who should no longer have access will gain unauthorized access to information and systems, NIST provides guidance for monitoring network accounts and identity management.

OAs Do Not Disable All Network Accounts as Required by DOT's Cybersecurity Policy

DOT's cybersecurity policy requires system administrators to close user accounts after separation from DOT or if the account is inactive for 90 days. We found 57 user accounts had not been disabled after the users had separated from DOT (see table 7). Three accounts had belonged to employees who were deceased. OAs disabled many accounts after we notified them of their status.

Table 7. Summary of Accounts that Were Not Disabled as of June 30, 2015

User Account Status by OA	> 365 Days	> 120 Days	> 90 Days	Total
FAA	1	3	1	5
FHWA	4	7	0	11
FMCSA	0	3	0	3
FRA	1	0	1	2
FTA	1	0	0	1
NHTSA	4	0	1	5
MARAD	4	1	0	5
OST	6	10	0	16
SLSDC	0	1	0	1
USMMA	8	0	0	8
Total	**29**	**25**	**3**	**57**

Source: OIG Analysis

In addition, a privileged account created for an OIG employee remained active for more than 2 years after the employee departed.[20] A privileged user is authorized and trusted to perform security-relevant functions that ordinary, or unprivileged,[21]

[20] The account was closed after we reported it to COE management.
[21] An unprivileged user uses an account for everyday access to applications such as email and data processing.

users are not authorized to perform. This account was created during the OIG's 2013 COE audit[22] to allow for penetration tests and vulnerability assessments to demonstrate weaknesses in the COE's network environment.

DOT Does Not Adequately Perform Periodic Reviews of Service Accounts

System administrators also need to disable inactive service accounts—which are not associated with a particular individual but are used to access system resources—that are no longer required. Not all OAs have completed this process. Specifically, 826 service accounts—including those FAA defines as special-use accounts, which are used to access systems or resources for specific needs—were inactive for longer than 90 days (see table 8).

Table 8. Summary of Account Activity as of May 2015

General Support System	Accounts	Accounts Inactive for over 90 days
COE	12,950	607
FAA	52,200	110
OIG Infrastructure	489	6
STB LAN	171	12
USMMA LAN	1,454	30
Volpe Center LAN	242	61
Total	67,506	826

Source: OIG Analysis

Of its 607 inactive accounts, COE did not identify which ones should remain active or be disabled. Last year, we informed COE about 584 inactive accounts we found during our review; COE did not provide a formal response at that time either.

After we notified the Department of our findings, FAA, USSMA, and Volpe reported taking corrective actions, including disabling a number of inactive accounts.

[22] *Security Weaknesses in DOT's Common Operating Environment Expose its Systems and Data to Compromise*, OIG Report Number FI-2013-123, September 10, 2013.

FAA NAS Networks Are Not Monitored by the CSMC, and Some Incidents Have Gone Unreported

Under FISMA, OMB policy, and NIST guidelines, Departments must establish an incident response and reporting program for their information systems. According to DOT, when an incident such as a security breach or interruption of service occurs, the OA reports it to CSMC, which analyzes reports, categorizes each incident by type, and reports incidents to US-CERT. DOT policy requires CSMC to have full network visibility over all DOT systems, including systems operated on behalf of the OAs by contractors and other Government organizations.

As in prior years, CSMC does not have the ability to monitor all departmental networks—including some key FAA networks—for intrusions. Hence, CSMC relies solely on FAA self-reporting for the National Airspace System (NAS) environment. FAA does not comply with the Department's policy and does not have an internal policy for incident handling and response for air traffic control networks. As a result, DOT cannot provide assurance that all NAS security incidents were reported to CSMC, US-CERT, or law enforcement.[23]

CSMC's lack of a comprehensive view and monitoring of all departmental networks and devices exposes DOT's system to the risk of security breaches. Furthermore, monitoring gaps impede CSMC's ability to ensure that all incidents are reported to US-CERT as required by OMB and that the Department is mitigating all security incidents.

Some DOT Computers Do Not Meet the Required Security Level for Use of Commercial Software

OMB requires agencies to adopt USGCB settings for commercial software, including Microsoft Windows and Internet Explorer, which is commonly used across the Government. These configuration baselines provide the lowest acceptable level of system security and ensure the efficient use of resources. However, in our compliance testing of a statistical sample of 762 devices out of DOT's 83,621 active computers, OAs could not locate 400 of the sampled devices—devices that were listed in OA inventories. Based on our sample, we estimate that OAs could not find or test 44,523 computers,[24] or 53.2 percent of the universe of 83,621 computers that were active during compliance scanning.[25]

[23] We will provide further detail on these findings in our upcoming report on the Department's incident handling and response.
[24] Our estimate has a margin of error of +/-5.6 percentage points at the 90 percent confidence level.
[25] This estimate is an increase of approximately 2.5 percentage points from last year's 35,893 computers, or 50.7 percent of a universe of 70,753 active computers.

We scanned the 362 sampled computers with Windows that we could locate for compliance with USGCB settings. Based on this testing, we estimate that 85 percent of the controls for approximately 39,098 traceable computers in the Department's universe of 83,621 computers met baseline settings.[26] This is a slight decrease from 2014's 85.4 percent. See table 9 for a summary of the Department's overall USGCB compliance.

Table 9. Results of Sample Testing on USGCB for Windows Operating Systems for Available Systems

OA General Support Systems[a]	Computers Sampled	Controls Tested	Controls Passed	Controls Not Passed	Percent Passed
COE[b]	70	18,200	17,584	616	96.6
FAA LAN[c]	63	18,033	14,722	3,311	81.6
USMMA LAN	46	12,050	11,887	163	98.6
Volpe Center LAN[d]	42	10,804	8,962	1,842	82.9
STB LAN	61	15,921	14,632	1,289	91.9
OIG Infrastructure	80	20,880	20,839	41	99.8
Totals	**362**	**95,888**	**88,626**	**7,262**	

[a] OMB Circular A-130, Appendix III, defines a general support system as an interconnected set of information resources under the same direct management control that shares common functionality.

[b] The Department's consolidated IT network infrastructure that supports email, desktop computing, and network management. OIG received explanations for all deviations in non-compliant controls.

[c] FAA's consolidated network infrastructure.

[d] The Volpe Center reported that full compliance with USGCB settings was incompatible within its research and development and engineering environments, and noted that many of its workstations require special software for scientific and experimental purposes. For these systems, Volpe examines the USGCB security configuration for applicability where feasible and appropriate. Volpe has provided the appropriate deviations for non-compliant workstations.

Source: OIG analysis

Because the OAs cannot verify all computers comply with USGCB requirements, the Department cannot be sure that all computers with access to its information system networks are sufficiently protected from compromise. Computers that are vulnerable could also put DOT's mission and business operations at risk for compromise.

DOT Does Not Have a Comprehensive Risk Management Program

OMB requires agencies to implement risk management programs that include governance structures for managing and monitoring risk at three levels: enterprise,

[26] Our estimate has a margin of error of +/- 8.6 percentage points at the 90 percent confidence level.

business process, and system. FAA, FHWA, FRA, FTA, NHTSA, OIG, and PHMSA have developed their own programs, and provided us their internal risk management policies and procedures. These policies and procedures contained the appropriate elements, such as criteria for making risk based decisions. FMCSA, SLSDC, and STB reported they follow the DOT policy but have not established a program. MARAD and OST are in the process of developing agency management plans. The lack of maturity in the departmentwide risk management program makes it difficult for DOT to establish a structured process for managing the risks associated with its operations and the use of Federal information systems.

DOT Has Not Fully Implemented Its Process for Tracking Contractor Security Training

FISMA requires agencies to develop and maintain a comprehensive security training program that ensures all computer users are adequately trained in their security responsibilities before they are allowed access to agency information systems. Furthermore, both FISMA and OMB require agencies to provide basic security awareness training to employees and contractors who never access computer systems as well as to those who do. However, as we have previously reported, DOT lacks a system to effectively track contractors working for the Department and determine whether they have received required training. This ongoing weakness increases the risk that contractors will become victims of social engineering or commit acts that compromise the Department's information security.

DOT'S SYSTEM-LEVEL CONTROLS ARE NOT SUFFICIENT TO KEEP SYSTEMS SECURE OR ENSURE THEIR RECOVERY

The Department's system-level controls remain insufficient to protect its systems' security and ensure that the systems can be recovered in the event of a serious breach. Not all OAs comply with DOT's policy to implement NIST's risk management framework, which calls for up-to-date system authorization and contingency plans. OAs noncompliance is due in part to DOT's failure to establish a sufficient process for on-going system authorization and for monitoring common security controls. Furthermore, FAA has not categorized all of its contractor-operated systems according to the Department's policy. Last, OAs that use cloud computing have made little progress on compliance with security requirements.

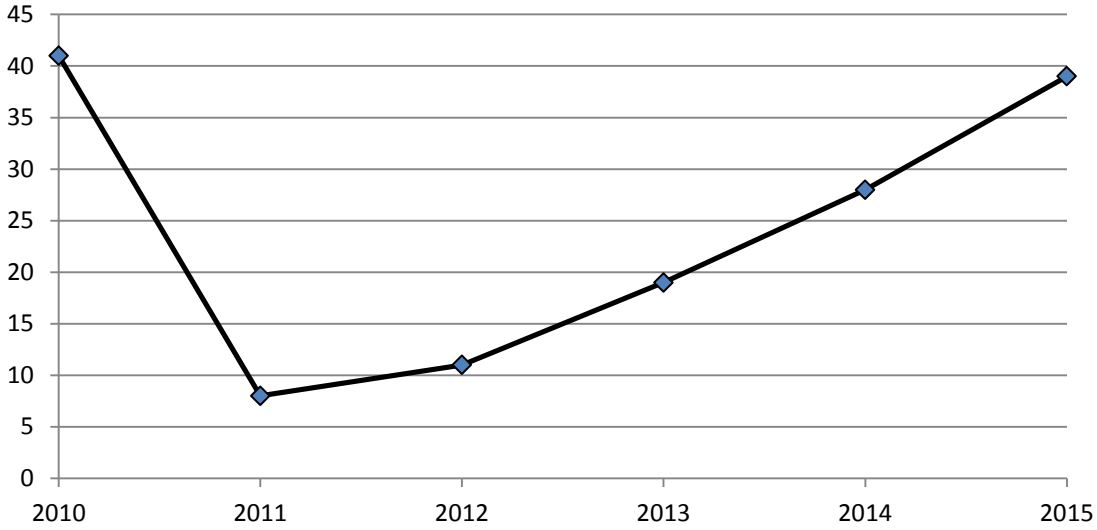
Some OAs Have Not Implemented NIST's Risk Management Framework

FISMA requires agencies to ensure all their information systems are secure to an acceptable level of risk. NIST's risk management framework helps agencies comply with this requirement by providing guidance for implementing, assessing, and monitoring the appropriate controls to identify and manage risks associated with their systems. The risk management framework includes several aspects of a security program: system reauthorization to operate; coordination of common controls; periodic testing of security controls; and contingency planning and testing. While DOT policy requires OAs to implement NIST's risk management framework, not all have done so.

Some OAs' Systems Operate with Expired Authorizations and without Evidence of Pending Reauthorization

(~~FOUO~~) OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires Federal agencies to authorize their systems at least once every 3 years. An authorizing officer, usually a senior executive, reviews certification results and reauthorizes the system when he or she determines that the system's operation poses minimal security risk. However, in 2015, 39 of DOT's systems' authorizations to operate had expired—compared to 8 in 2011 (see figure 1) [redacted]. Of the 39 systems, 20 have been unauthorized for multiple years. For example, OST has 4 systems that have not been authorized in the past 4 years. OAs also did not provide plans in CSAM for addressing lapses in authorization.

Figure 1. Expired Authorizations to Operate Over the Past 6 Years



Source: CSAM and OIG analysis

OAs' information security system managers have not provided authorizing officials with the required information for making risk-based decisions for reauthorization. For example, POA&Ms did not have reported or updated information, and authorizing officials authorized extensions to operate without supporting justification. See table 10 for the list of expired authorizations to operate by OA as of June 30, 2015.

~~(FOUO)~~ Table 10. Systems Overdue for Reauthorization

OA	Asset Reported as Outstanding for Reauthorization	[redacted]	Total
FAA	Office of Airports Local Area Network		7
	AST Local Area Network		
	Investment Planning and Management		
	Air Route Surveillance Radar Models 1 & 2		
	Air Transportation Oversight System		
	Overflight Fee Collection System		
	Access Key Credentialing System		
FHWA	Delphi Interface Maintenance System		3
	Fiscal Management Information System		
	Rapid Approval & State Payment System		
FMCSA	Electronic Document Management System		8
	Enforcement Management Information System		
	Hazardous Material Package Inspection Program		
	Licensing & Insurance		
	Performance & Registration Information Systems Management		
	FMCSA LAN Segment at Volpe		
	FMCSA Portal		
	SAFETYNET		
MARAD	BlackBoard		3
	Comprehensive Academic Management System		
	USMMA LAN		
NHTSA	PRISM		5
	NHTSA Inventory System		
	Crash Test Database		
	Traffic Records Improvement Program Reporting System		
	WEB System		
OST	Case Tracking System		13
	RITA Mission Support		
	RITA Web		
	Transtats		
	Airline Reporting Data Information System		
	Confidential Close Call Reporting System		
	Correspondence Control Management System		
	Civil Rights DBE and Airport Concession Ineligibility Database		
	External SharePoint[b]		
	Investigative Tracking System		
	Library Systems		
	Web Printing System		
	Workman Compensation Information System		
Total			**39**

[redacted]

[b]OST has reported this system as Retired, but has not provided evidence to support this.
Source: OIG analysis

Furthermore 19 of 24 sample systems had incomplete authorization documentation (see table 11).

Table 11. Sample Systems' Security Authorizations and Control Testing

OA	Systems Tested	Systems Without Adequate Security Authorization
FAA	12	11
FHWA	1	0
FMCSA	1	1
FRA	1	0
FTA	1	1
MARAD	1	1
NHTSA	1	1
OIG	1	1
OST	3	2
PHMSA	1	0
SLSDC	0	0
STB	1	1
Total	**24**	**19**

Source: OIG analysis

DOT's Process for On-Going System Authorization Is Insufficient

DOT policy requires each OA to have a plan for its systems' on-going authorization that outlines security control testing over a 3-year period. After authorizing officials first authorize and approve information systems' security posture, OAs are required to continually assess their systems' security status and sufficiently document system security plans, POA&Ms to resolve vulnerabilities,[27] and other information that relates to system security.

These documents, which are to be updated at least annually, inform authorizing officials risk-based decisions on systems' continued operation. However, in our

[27] POA&Ms and information on remediation and costs are stored in CSAM.

sample of 24 systems, we identified the following deficiencies in OAs' security posture documentation:

- For 19 systems, OAs did not provide evidence that security control tests complied with their plans for on-going authorization.
- For 19 systems, OAs did not perform required security control testing on common controls.
- For 7 FAA systems, the Agency's re-authorizations were based on incomplete security control testing and therefore inconsistent with the Agency's reauthorization plan.
- For 3 FAA NAS systems, customizations at different locations where the system operated were not tested. For example, the Alaskan Satellite Telecommunications Infrastructure system is deployed at 63 sites. The system is customized for use at each of these sites. However, FAA monitors these systems for reauthorization at only one location.

These deficiencies occur because OAs are not following applicable departmental guidance. The lack of effective on-going security monitoring for system re-authorization makes it difficult for authorizing officials to make effective risk-based decisions.

DOT's Procedures for Monitoring Common Security Controls Are Also Insufficient

Since 2012, we have reported that DOT lacks an effective process for OAs to assess, authorize, and monitor common security controls—controls that support multiple information systems. NIST requires providers[28] of these controls to (1) have policies and procedures for their use; (2) document the controls in separate security plans; (3) conduct ongoing assessment of the common controls' security, and monitor their effectiveness; and (4) inform users when changes occur that may adversely affect the protections provided by or expected of these controls.

While DOT recently developed common controls policy and procedures for its systems, except FAA's, the procedures lack practices for monitoring and authorizing these controls. FAA reported that it is in the process of developing an FAA-wide common control policy and practice guide but did not provide a scheduled implementation date.

[28] A provider is anyone that has a system control used by another system.

This lack of comprehensive policies and procedures and effective oversight of common controls could result in security incidents going undetected, unreported, or unresolved.

Several OAs Do Not Maintain Up-to-Date Contingency Plans

DOT policies require OAs to test and update their system contingency plans at least annually. A contingency plan, which contains detailed guidance and procedures for restoring a system after an unplanned shutdown, must be tested to validate its recovery capabilities, and updated regularly so it remains current with system enhancements and organizational changes.

However, for our 24 sample systems, 6 OAs had deficiencies in contingency planning and testing for at least 1 system[29] (see table 12).

Table 12. Summary of Deficiencies in Contingency Planning and Testing for Sample Systems

Contingency Planning Requirements	FAA	FMCSA	MARAD	NHTSA	OST	STB
Business Continuity and Disaster Recovery Plan (BCDRP)	X	✔	X	✔	✔	X
BCDRP revised to correct deficiencies found during testing	X	X	X	X	X	X
Contingency plans tested	X	X	X	✔	X	X
Contingency test after-action report developed	X	X	X	✔	X	X
System backup in accordance with procedures	X	X	X	✔	X	✔
Alternate processing sites defined	X	X	X	✔	X	X
Business Impact Analysis incorporated into COOP, BCP, DRP	X	X	X	✔	✔	X

Source: OIG analysis

A lack of effective contingency planning makes it difficult for the Department to recover its systems in the event of an unplanned service disruption—some of which can have devastating effects on DOT's number one mission: safety. For example, on September 26, 2014, an FAA contract employee deliberately started a fire that destroyed critical telecommunications equipment at FAA's Chicago Air Route Traffic Control Center in Aurora, IL. As a result of the damage, Chicago

[29] We reviewed additional systems as part of a separate contingency planning audit, and will provide further details on these systems in our report on that audit.

Center was unable to control air traffic for more than 2 weeks, thousands of flights were delayed or cancelled, and aviation stakeholders and airlines reportedly lost over $350 million.

FAA Has Not Categorized All of Its Contractor-Operated Systems

As required by OMB, agencies' asset inventories must identify who manages each system—the agency or an outside entity—and designate each accordingly, as organization operated or contractor operated.[30] However, in 2014, we reported that FAA had mislabeled 86 systems as non-contractor operated; at this writing, the Agency has not taken action to correct this. According to FAA, the 86 systems should not be classified as contractor systems, but it did not provide a justification for not changing their classifications.

Contractor systems present unique risks because the Department frequently does not manage these systems' security controls. The lack of an accurate system inventory makes it difficult for DOT to provide direction to OAs and contractors on information security, to enforce compliance with information security requirements, and to ensure security risks are reduced.

OAs that Use Cloud Computing Do Not Comply with Requirements

Cloud computing provides convenient access to computing resources that can be rapidly provisioned and released, including networks, servers, storage, and applications. Cloud computing resources are either private—for a single organization's exclusive use—or public, with infrastructure open to the general public. OMB requires agencies to identify all information systems that use cloud computing and ensure that the systems adhere to Federal cloud computing security requirements. These requirements are documented in OMB's Federal Risk and Authorization Management Program (FedRAMP). OMB's templates help agencies satisfy FedRAMP's requirements with standard language for contracts and service agreements with providers.

During a recent review of cloud services within DOT,[31] we found issues similar to ones we reported in prior FISMA audits. Specifically, FHWA, FAA, FRA, OST, and NHTSA could not provide evidence of their compliance with requirements. FMCSA reported that it had incorporated contract language for its cloud service provider acquisition, but it developed this language independently because DOT

[30] Contractor operated systems are either fully or partially owned or operated by a contractor, another agency, or other entity.
[31] *DOT Lacks An Effective Process for Its Transition to Cloud Computing*, OIG Report Number FI-2015-047, June 16, 2015.

lacked guidance. Furthermore, cloud systems at FAA, FRA, MARAD, and OST were not compliant with FedRAMP's requirements, which states that a specific set of security controls be implemented and that the responsibility for each set—agency personnel or cloud service provider—be specified.

Furthermore, DOT does not maintain a reliable inventory of cloud based systems, and has not reviewed existing cloud computing agreements to assess compliance with DOT policy, including security requirements. The lack of accurate inventories of IT investments that use cloud services makes it difficult for the Department to ensure that cloud computing agreements comply with FedRAMP requirements, thus placing systems at risk for compromise.

DOT AND OAS DO NOT REMEDIATE SECURITY WEAKNESSES ACCORDING TO ALL REQUIREMENTS

Federal agencies must comply with several requirements to remediate security weaknesses:

- FISMA requires agencies to develop processes to remediate security weaknesses.
- OMB requires departments to develop POA&Ms for system weaknesses and to prioritize remediation based on the seriousness of each weakness.
- DOT policy requires OAs to categorize their systems' weaknesses as low, medium, or high priorities based on OAs' criteria and to record POA&Ms in the CSAM repository. Untracked or unresolved POA&Ms make it difficult for DOT to ensure systems are secured and protected.

However, the CSAM repository is not complete. FAA did not establish POA&Ms for control weaknesses identified in over 150 audit recommendations for addressing significant security weaknesses in its air traffic control information security program that GAO made in 2015.[32] As of September 30, 2015, none of these recommendations have been closed. OCIO informed us that FAA is independently tracking these weaknesses and would not be able to fully remediate until the end of fiscal year 2018. Our 31 recommendations are also missing from CSAM and remain open. Furthermore, OAs have not recorded POA&Ms in CSAM on security weaknesses found during system scans for vulnerabilities. For 16 of 24 sample systems, OAs did not include information on all identified security weaknesses in CSAM. An incomplete central POA&M repository

[32] GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221, January 2015.

prevents DOT's CIO and Chief Information Security Officer from having timely and complete data to assess risk and funding requirements, analyze trends pertaining to weaknesses, and implement departmentwide solutions.

OAs have 3,830 open POA&Ms—a reduction of 1,798 (32 percent) from 2014—some of which date from 2009. In addition, we noted the following issues with the 3,830 reported POA&Ms:

- 2023 POA&Ms do not have actual start dates—in some cases, the OAs reported the planned start dates in CSAM but did not start remediation work on the planned dates and did not update the information with new dates. Of the 2023 POA&Ms, 188 are high priority, and 1569 are medium priority; and
- 960 POA&Ms—53 high, 316 moderate, 534 low, and 57 not categorized—had no documented remediation costs.

Table 13 provides details on the 3,830 POA&Ms reported by OAs.

Table 13. Summary of POA&Ms Opened between 2009 and 2014 without Actual Start Dates or Documented Remediation Costs, by OAs

OA	Total Open POA&Ms	With Actual Start Date mark as "TBD"	No Documented Cost
FAA	1780	1307	487
FHWA	71	69	0
FMCSA	884	3	11
FRA	137	88	26
FTA	269	0	0
MARAD	329	323	260
NHTSA	20	20	20
OIG	11	4	9
OST	243	162	102
PHMSA	18	10	0
SLSDC	9	1	1
STB	59	36	44
Total	**3830**	**2023**	**960**

Source: CSAM POA&M report as of October 8, 2015

CONCLUSION

Maintaining a secure information network is critical to ensuring operations across the Government are carried out efficiently and effectively. For DOT, secure systems are also critical to ensuring public safety—the Department's foremost mission. While DOT has made significant progress in implementing PIV, we continue to find that many of its information security controls are deficient. In some security areas, such as authorizing systems to operate, deficiencies are increasing. Until DOT takes action to remediate these deficiencies and puts in place the comprehensive policies and procedures needed to maintain the confidentiality, integrity, and availability of its data and systems, the Department's information systems will continue to be at increased risk of attack or compromise.

RECOMMENDATIONS

To help the Department address the challenges in developing a mature and effective information security program, we recommend that the Deputy Secretary, or his designees, take the following actions in addition to the 31 recommendations that are still open from prior FISMA reports.

1. Ensure that the OCIO revises the Departmental policy to document its practice of prohibiting user-based waivers or exclusions for PIV required use for network and system access.

2. Work with the OAs to develop a formal transition plan to the proposed ISCM target architecture that includes but is not limited to: (1) continuously assessing security controls; (2) reviewing system configuration settings; and (3) assessing timely remediation of security weaknesses. During the transition period, establish processes and practices for effectively collecting, validating, and reporting ISCM data. .

3. Ensure that FAA, FHWA, FMCSA, FRA, FTA, NHTSA, MARAD/USMMA, OST, and SLSDC perform actions to immediately disable user accounts that have been inactive for over 90 days, as required by the DOT compendium. Report completion of this effort to OCIO. Create a POA&M to track progress and verify completion of the action.

4. Work with OAs to develop internal controls to ensure network administrators are informed and action is taken to disable accounts when users no longer require access.

5. Work with the OCIO to develop a quality assurance process to ensure OAs and network administrators are following DOT Cybersecurity procedures that require them to periodically review user accounts and ensure they are effectively managing these accounts.

6. Revise DOT's existing Cybersecurity policy to incorporate specific requirements for review and cleanup of service accounts.

7. Work with the COE's management to ensure review and cleanup activities of service accounts are successfully completed.
8. Work with FAA to improve its assessment process to meet DOT Cybersecurity Compendium and Security Authorization & Continuous Monitoring Performance Guide. DOT CIO in conjunction with the FAA CIO review the FAA quality assurance process to ensure all security documents are reviewed and updated to reflect the system controls, vulnerabilities, and that the current risks are clearly presented to the authorizing officials.

9. Work with the OAs to ensure they update open POA&Ms with the required data fields.

AGENCY COMMENTS AND OIG RESPONSE

We provided the Department with our draft report on October 19, 2015, and received its response—included as an appendix to this report—on October 30, 2015. The Department generally concurred with all nine recommendations. However, the Department did not provide specific information on its planned actions or completion dates as requested in our draft report, we consider those recommendations open pending completion of the planned actions. Therefore, until we receive this information, we will consider them open and unresolved.

ACTIONS REQUIRED

We consider all 9 recommendations open and unresolved. In accordance with DOT Order 8000.1C, we request that the Department provide, within 60 days of this report, the additional information requested above regarding its specific actions taken or planned for each recommendation.

We appreciate the courtesies and cooperation of the Department's representatives during this audit. If you have any questions concerning this report, please call me

at (202) 366-1959, or Louis C. King, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

cc: Assistant Secretary for Budget and Programs/Chief Financial Officer
CIO Council Members
DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

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

Generally accepted Government auditing standards also require us to disclose impairments of independence or any appearance thereof. OMB requires that the FISMA template include information from all OAs, including OIG. Because OIG is a small component of the Department, based on number of systems, any testing pertaining to OIG or its systems does not impair our ability to conduct this mandated audit.

FISMA requires us to perform annual independent evaluations to determine the effectiveness of DOT's information security program and practices. FISMA further requires that our evaluations include testing of a subset of systems, and an assessment, based on our testing, of the Department's compliance with FISMA and applicable requirements.

To meet FISMA and OMB requirements, our objective would determine the effectiveness of DOT's information security program and practices for the 12-month period between July 1, 2014, and June 30, 2015. Per OMB's Annual Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, agencies should set cut-off dates for data collection and report preparation that allow adequate time for meaningful internal reviews, comments, and resolution of disputes before reports' finalization. The OCIO agreed to use a cutoff of June 30. We assessed a subset of 24 of 463 departmental systems and reviewed the compliance of these systems with NIST and DHS requirements in the following areas: risk categorization; security plans; annual control testing; contingency planning; certification and accreditation; incident handling; and plans of actions and milestones. See table 14 for sampled systems and table 16 for the system inventory. Of the systems selected for review, 24 were available but one had a name change. Our random selection was based on a universe of 379 systems that had not been reviewed in 3 years. To evaluate USGCB compliance, we selected a statistical sample of 762 of 83,621 devices to

scan for compliance. We created a script to extract the test results of USGCB controls from 362 of 762 devices that were available for scanning.

We evaluated prior years' recommendations and supporting evidence to determine what progress had been made in the following areas: continuous monitoring; configuration management; contingency planning; risk management; security training; contractor services; and identity and account management. We also conducted testing to assess the Department's device inventory; its process for resolution of security weaknesses; configuration management; incident reporting; security awareness training; remote access; and account and identity management. Our tests included analyses of data contained in CSAM, reviews of supporting documentation, and interviews with departmental officials.

As required, we submitted to OMB qualitative assessments of DOT's information security program and practices. We performed our information security review work between April and November 2015. We conducted our work at departmental and OA Headquarters' offices in Washington, D.C.

Table 14. OIG's Representative Subset of DOT Systems by OA

(~~FOUO~~) System		Impact Level[a]	[redacted]	Contractor System[c]
Federal Aviation Administration				
1	Overflight Fee Collection System (OFCS)	Moderate	[redacted]	N
2	Alaska Boundary Connection (ABC)	Moderate		N
3	Enterprise Services Center Cloud Enclave	Moderate		N
4	AIT Office of Information & Technology Headquarters Enterprise Data Center (AIT HQ EDC)	Moderate		N
5	Automated Vacancy Information Access Tool (AVIATOR)	Moderate		N
6	Access Key Credentialing System (AKCS)	Moderate		N
7	Certification & Compliance Management Information System.Net (CCMISNet)	Moderate		Y

FOR OFFICIAL USE INFORMATION WAS REDACTED FOR PUBLIC RELEASE

	(~~FOUO~~) System	Impact Level[a]	[redacted]	Contractor System[c]
8	Recovery Communications System (RCOM)	Moderate		N
9	Aeronautical Mobile Communications System (AMCS)	Moderate		Y
10	Alaskan Satellite Telecommunications Infrastructure (ASTI)	Moderate		N
11	Business Continuity Support System (BCSS)	Moderate		N
12	Air Transportation Oversight System (ATOS)	High		N
Federal Highway Administration				
13	Transportation Fellows Interns & Contractor System (TFICS)	Moderate		Y
Federal Motor Carrier Safety Administration				
14	FMCSA LAN Segment at Volpe	Moderate		N
Federal Transit Administration				
15	Transportation Electronic Award Management System	Moderate		Y
Federal Railroad Administration				
16	Railroad Network System	Moderate		Y
Maritime Administration				
17	Cargo Preference Overview System	Moderate		Y
National Highway Traffic Safety Administration				
18	Support Delivery Services Low Impact System (SDSLIS)	Low		Y
Office of Inspector General				
19	US Department of Transportation/Office of Inspector General (US DOT/OIG)	Moderate		N

FOR OFFICIAL USE INFORMATION WAS REDACTED FOR PUBLIC RELEASE

(~~FOUO~~) System		Impact Level[a]	[redacted]	Contractor System[c]
Pipelines and Hazardous Materials Safety Administration				
20	Pipeline Risk Management Information System (PRMIS)	Low	[redacted]	Y
Office of the Secretary of Transportation				
21	Enterprise Support Systems (ESS)	Moderate	[redacted]	N
22	Volpe Physical Access Control System (VPACS)	High		Y
23	Common Operating Environment (DOT COE)	High		Y
Surface Transportation Board (STB)				
24	Local Area Network (LAN)	Moderate	[redacted]	N

Legend: N = No Y = Yes

[a] NIST defines impact levels based on the effect a breach of security could have on a system's confidentiality, integrity and availability. If the effect is limited, the impact level is low; if serious, moderate; if severe, high.

[redacted]

[c] DOT's definition of contractor system.

Source: OIG analysis

Our previous reports issued in response to FISMA's mandate are:

- *DOT has Made Progress but Significant Weaknesses in its Information Security Remain*, OIG Report Number FI-2015-009, November 14, 2014.
- *DOT Has Made Progress, But Its Systems Remain Vulnerable To Significant Security Threats*, OIG Report Number FI-2014-006, November 22, 2013.
- *Ongoing Weakness Impede DOT's Progress Toward Effective Information Security*, OIG Report Number FI-2013-014, November 14, 2012.
- *Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information Systems*, OIG Report Number FI-2012-007, November 14, 2011.
- *Timely Actions Needed to Improve DOT's Cybersecurity*, OIG Report Number FI-2011-022, November 15, 2010.
- *Audit of DOT's Information Security Program and Practices*, OIG Report Number FI-2010-023, November 18, 2009.

Exhibit A. Scope and Methodology

- *DOT Information Security Program*, OIG Report Number FI-2009-003, October 8, 2008.
- *DOT Information Security Program*, OIG Report Number FI-2008-001, October 10, 2007.
- *DOT Information Security Program*, OIG Report Number FI-2007-002, October 23, 2006.
- *DOT Information Security Program*, OIG Report Number FI-2006-002, October 7, 2005.
- *DOT Information Security Program*, OIG Report Number FI-2005-001, October 1, 2004.
- *DOT Information Security Program*, OIG Report Number FI-2003-086, September 25, 2003.
- *DOT Information Security Program, OIG Report Number* FI-2002-115, *September 27, 2002.*
- *DOT Information Security Program, OIG Report Number* FI-2001-090, *September 7, 2001.*

Exhibit A. Scope and Methodology

FOR OFFICIAL USE INFORMATION WAS REDACTED FOR PUBLIC RELEASE

EXHIBIT B. Previous Years' Open Recommendations

Table 15. Summary of Open Recommendations, Fiscal Years 2014-2009

Fiscal Year 2014; OIG Report Number FI-2015-009	
Number	**Recommendation**
1	Revise the Department's AECM policy to develop procedural requirements that document activities components must complete to report and mitigate deficiencies identified through continuous monitoring.
2	Implement the revised AECM policy and procedural guidance and provide and work with components to establish planned action dates to mitigate deficiencies in their ISCM reporting and addressing security weaknesses.
3	Establish an enterprise-wide strategy that DOT components must adhere to implement and monitor Information Security Continuous Monitoring for Continuous Diagnostics and Mitigation requirements as outlined in OMB policy and NIST guidance.
4	Revise the Department's policy to address the mandatory use of a toolset and requisite processes to perform the Information Security Continuous Monitoring tasks outlined by OMB.
5	Start planning and assessing impact of the security requirements that will be affected by NIST SP 800-53 revision 4 and NIST SP 800-53A revision 4.
6	Revise DOT Cybersecurity policy and guidance to incorporate new or updated security requirements defined by NIST SP 800-53 revision 4 and NIST SP 800-53A revision 4.
7	Work with components to develop a plan to address NIST 800-53 revision 4 requirements for their systems. Create a POA&M with a planned completion date to monitor and track progress.
8	Work with the components to develop a plan to complete annual SAT training within plan milestones. Assess training periodically to determine if the component will meet SAT training plan.
9	Work with the FAA to ensure automated scripts are properly configured to disable inactive user accounts in a timely manner. Create a POA&M with a planned completion date to monitor and track progress.
10	Work with the CSMC and individual components (including COE) to develop service level agreements needed to define responsibilities between CSMC and the components. These agreements should include a detailed description of services between parties, at a minimum contain: CSMC and component responsibilities; frequency of periodic scans of DOT networks; access privileges to networks, devices, and monitoring tools; hardware and software asset discovery and on-going management requirements; vulnerability scanning.
11	Revise DOT policy to provide specific guidance for what data, format of data, and how often components should report system security status to the

FOR OFFICIAL USE INFORMATION WAS REDACTED FOR PUBLIC RELEASE

	Authorizing Official throughout the continuous monitoring process.
12	Work with FAA to revise their plan to effectively transition the remaining 32,266 users to require unprivileged PIV login. Create a POA&M with a planned completion date to monitor and track progress.
15	Work with components to develop or revise their plans to effectively transition the remaining information systems to required PIV login. Create a POA&M with a planned completion date to monitor and track progress.
16	Work with the Director of DOT Security to develop or revise their plans to effectively transition the remaining facilities to required PIV cards.

Fiscal year 2013; OIG Report Number FI-2014-006

Number	Recommendation
1	Obtain and review specialized training statistics and verify, as part of the compliance review process, that all employees with significant security responsibilities have completed the number of training hours required by policy. Report results to management and obtain evidence of corrective actions.
2	Increase oversight of OAs processes for configuration management and verify that mitigating activities and initiated, executed, and completed in accordance with DOT policy and NIST guidance. Report exceptions to OA management.
4	Obtain and review plans from FMCSA, MARAD, OST, and RITA to authorize systems with expired accreditations. Perform security reviews of unauthorized systems to determine if the enterprise is exposed to unacceptable risk.
5	Obtain a schedule and action plan from Operating Administrations to enhance and develop their internal procedures for continuous monitoring in accordance with NIST guidance. Report to OA management any delays in completing the procedural guidance.
6	Review systems to determine which ones are contractor operated and update CSAM accordingly. As part of the compliance review process, review new systems to determine if they are contractor operated.
7	Obtain a schedule and action plan for OAs to develop procedures for comprehensive cloud computing agreements to include security controls roles and responsibilities. Report to OA management any delays in completing the procedures.
8	Obtain and review existing cloud computing agreements to assess compliance with agency policy, including security requirements. Report exceptions to OA management.

Fiscal Year 2012; OIG Report Number FI-2013-014

Number	Recommendation
1	Work with Operating Administrations to enhance and develop their internal procedures for inheriting controls, continuous monitoring, and capital planning to better address key NIST requirements.
4	Develop, document and approve an enterprise-wide risk management program and strategy as defined by NIST 800-39.
5	Identify and work with common control providers to develop and implement a

Exhibit B. Status of Prior Years' Recommendations

	security plan that will ensure that systems that inherit common controls are adequately protected and C&A'd.

Fiscal Year 2011; OIG Report Number FI-2012-007

Number	Recommendation
1	Address these policy and procedural weaknesses: •Issue information security policy for OST. •Enhance existing policy to address security awareness training for non-computer users, address security costs as part of capital planning, correct the definition of "government system", and address the identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications. •In conjunction with the OA CIOs, execute a strategy to ensure that sufficient procedural guidance exists for DOT and the OAs.
4	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.
6	In conjunction with OA CIOs, verify that minimum security controls are adequately tested for deficient systems.

Fiscal Year 2010; OIG Report Number FI-2011-022

Number	Recommendation
14	Identify and implement automated tools to better track contractors and training requirements.
18	Review the results of OA assessments to determine an accurate inventory of contractor systems.

Fiscal Year 2009; OIG Report Number FI-2010-023

Number	Recommendation
16	Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.
20	Improve its quality assurance checks on the Operating Administrations' certifications and accreditations by increasing the frequency and scope of its checks, communicating results and expected actions to the Operating Administrations, requiring updated plan of actions and milestones to address weaknesses noted (including those found in the Inspector General reviews), and follow-up on resolution of weaknesses noted.

EXHIBIT C. DOT'S OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

(~~FOUO~~) Table 16. System Inventory Counts for Fiscal Years 2014 and 2015

Organization[a]	FY 2014	FY 2015
Federal Aviation Administration (FAA)	320	318
Federal Highway Administration (FHWA)	20	19
Federal Motor Carrier Safety Administration (FMCSA)	16	18
Federal Railroad Administration (FRA)	12	12
Federal Transit Administration (FTA)	6	8
Maritime Administration (MARAD)	19	17
National Highway Traffic Safety Administration NHTSA)	10	16
Office of Inspector General (OIG)	2	3
Office of the Secretary (OST)	44	43
Pipeline and Hazardous Materials Safety Administration (PHMSA)	7	7
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)[b]	1	1
Total Systems	**458**	**463**

[redacted]

[a] DOT includes the Office of the Secretary of Transportation (OST), the Office of the Inspector General (OIG), the Surface Transportation Board (STB), and 9 Operating Administrations: FAA, the Federal Highway Administration (FHWA), the Federal Motor Carrier Safety Administration (FMCSA), the Federal Railroad Administration (FRA), the Federal Transit Administration (FTA), the Maritime Administration (MARAD), the National Highway Traffic Safety Administration (NHTSA), the Pipeline and Hazardous Materials Safety Administration (PHMSA), the Saint Lawrence Development Seaway Corporation (SLDSC). In prior years, the Research and Information Technology Administration (RITA) was a separate component. RITA is now part of OST. For purposes of this report, we refer to OST, OIG, and STB as OAs.

[b] Under 49 U.S.C., Subtitle I, Chapter 7, in the performance of STB functions, the members, employees, and other personnel of the Board shall not be responsible to or subject to the supervision or direction of any officer, employee, or agent of any other part of DOT. Per the memorandum of understanding between DOT and COT, dated September 2013, STB is expected to operate in accordance with Federal and DOT policies to ensure the overall security and integrity of STB and COE networks.

Sources: CSAM as of July 14, 2015 and OIG analysis.

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis King	Assistant Inspector General for Financial and Technology Audits
Michael Marshlick	Project Manager
Maria Dowds	Senior Auditor
Martha Morrobel	Senior Information Technology Specialist
Tracy Colligan	Senior Information Technology Specialist
Jenelle Morris	Senior Information Technology Specialist
Jo'Shena Jamison	Information Technology Specialist
Antione Searcy	Information Technology Specialist
Petra Swartzlander	Senior Statistician
Makesi Ormond	Statistician
Karen Sloan	Communications Officer
Susan Neill	Writer-Editor

APPENDIX. AGENCY COMMENTS

Memorandum

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

SUBJECT: **ACTION**: Management Response to the OIG Draft Report—FISMA 2015: DOT Has Major Success in PIV Implementation, But Problems Persist in Other Cybersecurity Areas

DATE: October 30, 2015

FROM: /s/ Richard McKinney
DOT Chief Information Officer

Reply To Attn. of:

TO: Calvin L. Scovel III
Inspector General

The Department remains committed to improving its information security program. We are pleased that the Office of Inspector General (OIG) Federal Information Security Modernization Act (FISMA) 2015 report acknowledges improvements in the Department's use of personal identity verification (PIV) cards to secure network access for agency personnel and privileged network account holders. We have made progress over the past year and achieved a number of accomplishments to include the following:

- Recruited 6 new cybersecurity personnel in the Office of the Chief Information Officer (CIO), including the hiring of a new Chief Information Security Officer (CISO) for the agency.

- Reached or exceeded the Department's targets for Fiscal Year 2015 Cybersecurity Cross-Agency Priority goals: (1) monitored more than 95% of Transportation IT assets for hardware and software inventory using existing tools; (2) required 98.3% of unprivileged network accounts to authenticate to agency networks using their PIV cards; (3) required 100%

of privileged network accounts to authenticate to agency networks using their PIV cards; and (4) provided 100% coverage of agency e-mail with anti-phishing and anti-malware defensive capabilities.

- Collaborated with the Office of Security to identify funds for and acquire a new personnel security system in Fiscal Year 2015 that supports tracking of both Federal and contractor personnel, with full implementation planned for Fiscal Year 2016.

- Completed reviews of agency contracts covering the processing and storage of sensitive privacy information in collaboration with the Office of the Senior Procurement Executive.

- Successfully participated in and met the objectives of the Federal Cyber Sprint led by the Federal CIO and the Office of Management and Budget cyber team; and

- Participated in the evaluation and award of Task Order 2B Continuous Diagnostics and Mitigation (CDM) contracts with the General Services Administration and the Department of Homeland Security, and initiated CDM implementation across the agency to enhance the agency Information Security Continuous Monitoring (ISCM) program, and implement an agency risk management dashboard that will also provide information to DHS.

Additionally, we have initiated actions to remediate or address a number of issues the OIG identified previously or during this evaluation, to include the following:

- Identified positions and funding to fill existing vacancies within the DOT CISO's organization, and add up to 5 additional personnel to support cybersecurity program needs including security authorization and compliance, vulnerability management, and weakness/vulnerability remediation.

- Identified and remediated, upgraded, or retired desktop, laptop, and server systems running obsolete and unsupported versions of software and operating systems, and leveraged this effort to ensure deployment of monitoring agent software (e.g. BigFix, Microsoft System Center Configuration Manager (SCCM), SolarWinds) on devices connected to the

Common Operating Environment (COE), and visibility into networks connected to the COE by the DOT Security Operations Center/Cyber Security Management Center.

- Completed and issued an updated agency IT strategic plan that includes a goal centered upon improving governance, compliance, and oversight, and a goal focused on a shared services strategy and model that increases and enhances the use of shared services, and common controls, for more consistent delivery of capabilities and improved security; and

- Initiated a network discovery and assessment activity by the Office of IT Shared Services to map and assess the non-FAA networks of the agency.

As we move forward, we will address the issues in the report based on Government-wide priorities, DOT strategic initiatives, data available from the Department's own monitoring and risk management systems, the OIG's work and recommendations, and available resources. The Department intends to use all tools at its disposal to address these matters and continue to holistically and cost-effectively improve its cybersecurity posture.

We provided our technical comments to the draft report to you separately. We generally agree with the recommendations in the draft report and within 60-days of the final report, we will provide you a specific response to each recommendation that identifies and prioritizes actions planned and anticipated milestones. Please contact me with any questions.