Office of Inspector General

Audit Report

FISMA 2014: DOT HAS MADE PROGRESS BUT SIGNIFICANT WEAKNESSES IN ITS INFORMATION SECURITY REMAIN

Department of Transportation

Report Number: FI-2015-009

Date Issued: November 14, 2014

Memorandum

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

Subject: **ACTION:** FISMA 2014: DOT Has Made Progress but Significant Weaknesses in Its Information Security Remain
Report Number: FI-2015-009

Date: November 14, 2014

From: Calvin L. Scovel III C. L. Scovel III
Inspector General

Reply to Attn. of: JA-20

To: Deputy Secretary

The Department of Transportation's (DOT) operations rely on 458 information technology (IT) systems, nearly two-thirds of which belong to the Federal Aviation Administration (FAA). 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 systems manage approximately $90 billion in Federal funds annually, including awarding and disbursing these funds.

To protect Federal IT systems, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement 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). Recently, an FAA contractor allegedly started a fire in a Chicago air traffic facility that disrupted system operations and caused delays and cancellations of hundreds of flights. A weak information security program can create gaps in the physical security and continuity of operations at air traffic control facilities that may contribute to this sort of incident.[1]

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices

[1] On October 15, 2014, OIG initiated an audit to review the Federal Aviation Administration's (FAA) contingency plans and security protocols at Chicago air traffic control facilities. OIG reports are available on our Web site at: www.oig.dot.gov.

for the 12-month period between August 1, 2013 and July 31, 2014.[2] Specifically, we assessed DOT's (1) information security policy and procedures; (2) enterprise-level information security controls;[3] (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 2014 FISMA reporting metrics, we assessed 20 sample systems, and performed analytical reviews of data contained in the Department's Cybersecurity Assessment and Management system (CSAM).[4] We also tested software settings in 6 general support systems, reviewed supporting documentation, and interviewed Department officials. As part of this work, we selected a statistical sample 756 devices out of 70,753 active computers that allowed us to project that 85.4 percent[5] of DOT's computers are compliant with configuration standards.[6] See exhibit A for details on our scope and methodology. Also, as required by OMB, we provided our results to OMB via its Web portal.[7]

RESULTS IN BRIEF

Since our 2013 review, DOT has made progress towards compliance with FISMA requirements in its information security program. For example, the Department reported increased network traffic through the trusted internet connections (TIC)[8] from 55 percent to 74 percent. It reported that 99 percent of departmental traffic is currently flowing through the TIC. The Department has also taken steps to improve its deployment of personal identity verification cards, and improved compliance with configuration standards. However, the Department's information systems remain vulnerable to serious security threats due to the following deficiencies.

1. DOT's Office of the Chief Information Officer (OCIO) and operating administrations (OA) have not addressed all weaknesses we previously identified. Specifically, OCIO has not: (1) established comprehensive guidance

[2] Per OMB 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. Our audit covers the 12-month period ending on the cutoff date.

[3] For purposes of this report, enterprise-level controls include security training, incident response and reporting, capital planning and investment control, and configuration management, and are generally not system-specific.

[4] CSAM tracks system inventories, weaknesses, and other security information.

[5] Our estimate has a margin of error of +/-7.9 percentage points at the 90 percent confidence level.

[6] United States Government Configuration Baselines are security configuration settings developed by the National Institute of Standards and Technology (NIST), the Department of Defense, and Department of Homeland Security for certain Windows operating systems.

[7] Because OMB designates this information "For Official Use Only," our submission to OMB is not contained in this report.

[8] As outlined in OMB Memorandum M-08-05, a TIC optimizes and standardizes the security of individual external network connections that Federal agencies use, including connections to the Internet.

for the OAs to implement the automated enterprise continuous monitoring (AECM) program for effective cybersecurity monitoring; (2) OCIO and the OAs have also not finalized procedures, oversight and risk assessment for common security controls;[9] (3) DOT's policy and guidance do not address the hundreds of new controls and enhancements identified in National Institute of Standards and Technology's (NIST) Special Publication 800-53, revision 4, which covers implementation of security controls and requires agencies to assess new controls and enhancements for compliance to security requirements; and (4) DOT policy does not comply with NIST's guidance by allowing the OAs to test new controls within 2 years instead of 1. These gaps in DOT procedures have contributed to the security weaknesses we previously identified.

2. DOT's enterprise-level controls—controls that must be implemented across the Department—remain inadequate. Specifically, OAs do not: (1) effectively track contractors' completion of security awareness training; (2) meet requirements for specialized training for personnel with security duties; (3) provide agreements between Cybersecurity Management Center (CSMC) and OAs that clearly define the OAs' and Center's responsibilities for monitoring the network and devices so that monitoring gaps are avoided; (4) disable accounts after 90 days of inactivity in accordance with DOT policies; (5) monitor all network devices for compliance with the U.S. Government Configuration Baseline (USGCB); and (6) implement effective risk management program.[10] Lastly, the Department has not implemented an effective security capital planning program.

3. The Department's system-level controls also remain insufficient to protect system security. The OAs have not adhered to the Department's requirement to implement NIST's risk management framework,[11] and to identify and manage system risks. Specifically, the OAs have: (1) allowed expiration of systems' authorizations to operate; (2) not established effective procedures for monitoring common security controls; (3) not established continuous monitoring of security controls; (4) not completed implementation of access to information systems and facilities requiring use of personal identity verification (PIV) cards; and (5) not effectively planned for contingencies. FAA also has not established an accurate inventory of its contractor operated systems and six OAs do not accurately account for cloud computing systems in the Cybersecurity Assessment and Management database (CSAM), the central

[9] A control that is part of a network and used by a software application that resides on that network.

[10] Risk management programs include governance structures for managing and monitoring risk at three levels: enterprise, business process, and system.

[11] The risk management framework is a structured process or steps to assess risk during the system development life cycle. For example, the first step is the process is categorizing a system as high, medium, or low based on its impact.

repository that tracks system inventories, security weaknesses, and other security information.

4. The Department also still lacks sufficient management oversight of remediation of plans of action and milestones (POA&M) for identified system weaknesses. For 5,628 open POA&Ms, approximately 21 percent did not have planned start dates for remediation of the weaknesses, and almost 52 percent—including some that were moderate and high risk—did not document costs of remediation. Furthermore, the OAs do not report all security weaknesses in CSAM.

Policy and procedure deficiencies—absence or enforcement—contribute to the weaknesses we identified. Deficiencies in enterprise and system level controls, as well as slow remediation of security weaknesses, increase the risk that DOT's sensitive information and its systems may be compromised and that operations may be disrupted. We are making a series of recommendations to further assist the Department in establishing and maintaining an effective information security program—one that complies with FISMA, OMB, and other requirements. Tables 14 through 18 in exhibit B identify the open recommendations from our five previous FISMA reports.

BACKGROUND

FISMA requires each Federal agency to establish an information security program that secures 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 Government Accountability Office on the effectiveness of its information security policies, procedures, and practices.

DOT's 13 OAs manage the Department's 458 information systems. The Department relies on these systems to carry out its mission, including safe air traffic control operations, preventing unqualified drivers from obtaining commercial driver's licenses, and identifying safety defects in vehicles. DOT must also ensure the integrity of transaction data and reports that account for the billions of dollars used for highway reconstruction, high-speed rail development, and law enforcement grants.

For 2014, OMB required inspectors general to use 104 security metrics in 11 security areas to assess their agencies' performances. To put more emphasis on automated capabilities for information security continuous monitoring for this year's review—an administration priority[12]—OMB added 6 metrics—3 in area of continuous monitoring, 2 in configuration management, and 1 in remote access management.

Since 2001, we have published a series of 13 information security reports, as required by statute, evaluating weaknesses in DOT's information security program and practices. See exhibit A for a list of prior information security audit reports.

OCIO AND THE OAS HAVE PUT NEW INFORMATION SECURITY POLICIES IN PLACE, BUT OTHERS REMAIN INCOMPLETE

FISMA requires each Department's CIO to develop and maintain information security policies and procedures to address security requirements. Supporting guidance and procedures on how to effectively implement specific controls augment an agency's security policy. The Department CIO may also delegate to the 13 OAs the authority for creating procedures that comply with departmentwide policies. In response to our recommendations, OCIO issued its policy and required OAs to complete compliant procedures within 1 year. However, in 4 areas, neither OCIO nor the OAs have completed the required policies and procedures. See table 1 for details.

[12] Administration priorities are metrics for trusted internet connection capabilities and utilization, mandatory authentication and personal identify verification, and continuous monitoring.

Table 1. Deficiencies in Policies and Procedures

Security Program Area	OIG Evaluation
Continuous Monitoring of Controls	
Information Security Continuous Monitoring (ISCM) maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Processes that support ongoing security monitoring across an organization must include leadership's definition of a comprehensive ISCM strategy that encompasses technology, processes, procedures, operating environments, and people.	OCIO reported that its strategy for ISCM is the AECM program that DOT initiated in fiscal year 2012. AECM, however, lacks comprehensive guidance for implementation, monitoring, reporting, and enforcement for effective real-time cybersecurity monitoring.[13]
Personal Identity Verification	
Personal identity verification (PIV) is the governmentwide initiative to provide users of Federal networks with an ID card that uses smart-card technologies to control access to Federal facilities and resources.	OCIO has implemented a "waiver" program for OAs that have unique problems or challenges in meeting Federal PIV requirements. However, although OCIO has granted waivers, it has not finalized the policy that governs this process.
Risk Management	
For common controls, agencies must test controls, identify risks, determine whether they can accept the risks, and authorize the systems to operate.	OCIO and the OAs have not finalized their procedures for control testing and risk assessment for inherited 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

[13] Until recently, information systems were monitored for possible breaches and other incidents that may have occurred in the past. New technology allows for "real time" system monitoring.

In fiscal year 2013, OCIO's information security policy delegated authority to OAs to develop supplemental guidance on effective and consistent implementation of information security. We found that only 7 of 13 OAs had developed procedures specific to their needs. The CIO informed us that his office would review each OA's guidance to ensure that it aligns with the Department's policy. In fiscal year 2014, OCIO did not provide evidence that it had reviewed these policies. We also were not provided convincing evidence that OCIO was evaluating OA compliance with DOT's security program. For example, OCIO reported that it did not conduct a compliance review of FAA's information security program. In addition, OCIO noted that it had not conducted oversight of FAA. Both OCIO and the OAs have not finalized procedures for common controls oversight, ongoing risk determination, or ongoing risk acceptance decisions.

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

DOT CONTINUES TO LACK DEPARTMENTWIDE ENTERPRISE-LEVEL CONTROLS

DOT's enterprise-level controls—controls that must be implemented across the Department—remain inadequate. We noted deficiencies in training, monitoring networks for incidents, disabling inactive network accounts, configuring all department computers for required security level for commercial software use, and considering security costs when planning IT investments.

The Department Does Not Accurately Track Security Awareness Training for Contractors

FISMA requires agencies to develop and maintain a comprehensive security training program that ensures that all computer users, including contractors, are adequately trained in security responsibilities before they are allowed access to agency information systems. However, the Department still does not accurately track security awareness training completed by its contractors. According to DOT's senior officials, the Department has not implemented a tool capable of accurately tracking this training. With the current tracking process, the data collected by the OAs regarding which contractors have completed the training conflict with those collected by OCIO. For example, MARAD reported that it had 193 contractors while OCIO reported that MARAD had 492 contractors. See table 2 for a summary of the data from OICO and the OAs.

Table 2. Discrepancies between OCIO-Provided and OA-Provided Security Awareness Training Data

	Contractors Who Did Receive SAT			Contractors Who Did Not Receive SAT			Total number of Contractors Reported			Percent Contractor SAT Completion Rate		
OA	**OA Data**	**OCIO Data**	+/-	**OA Data**	**OCIO Data**	+/-	**OA Data**	**OCIO Data**	+/-	**OA Data**	**OCIO Data**	+/-
FAA	6861	6847	14	4408	4169	239	11269	11016	253	61	62	-1
FHWA	478	467	11	71	97	-26	549	564	-15	87	83	4
FMCSA	102	107	-5	17	36	-19	119	143	-24	86	75	11
FRA	112	114	-2	13	16	-3	125	130	-5	90	88	2
FTA	120	140	-20	22	4	18	142	144	-2	85	97	-12
MARAD	124	108	16	69	384	-315	193	492	-299	64	22	42
NHTSA	341	355	-14	74	78	-4	415	433	-18	82	82	0
OIG	47	N/A	N/A	0	N/A	N/A	47	N/A	N/A	100	N/A	N/A
OST	345	351	-6	48	41	7	393	392	1	88	90	-2
PHMSA	160	160	0	0	2	-2	160	162	-2	100	99	1
RITA/ VOLPE	393[b]	407[c]	-14	28[b]	**66**[c]	-38	421	473	-52	93	86	7
SLSDC	1	1	0	0	0	0	1	1	0	100	100	0

[a] STB reported they have no contractors.
[b] RITA did not provide data. The reported numbers are for VOLPE.
[c] This number includes RITA and Volpe. We were not informed how many contractors actually work for each OA.
Source: OIG analysis

This lack of regular security awareness training for contractors could result in behaviors that put DOT's information at risk, such as e-mail abuse, ID and password sharing and poor password development, and internet misuse.

Some OAs Do Not Require Personnel to Meet their Specialized Training Requirements

DOT's cybersecurity policy requires OAs to provide specialized security awareness training for personnel that perform certain security related roles. The policy specifies which roles require annual specialized training, defines the minimum number of hours required for each role, and provides guidance on industry-recognized certifications.

OCIO reported that it had made a change in its security policy that reduced the minimum number of hours of specialized training for certain roles. However, it did not provide a justification for this reduction. While some personnel completed training, the OAs do not meet the departmental requirement for specialized training. See table 3 for information on special training hours by OA.

Table 3. Specialized Security Training Summary

OA	Personnel Who Require Specialized Training	Personnel Who Met Department Requirements
FHWA	207	142
FTA	62	23
MARAD	28	4
NHTSA	54	0
RITA	Did not provide data	Did not provide data
SLSDC	3	0
STB	5	3

Source: OIG analysis

The lack of sufficient hours of specialized training for personnel with security related duties makes it difficult for DOT to be sure that that its personnel have the adequate knowledge, skills, and abilities consistent with their roles to protect the Department's information.

The Cybersecurity Management Center Does Not Monitor all of the Department's Networks and Devices

DOT's cybersecurity policy requires CSMC to have full network visibility for surveillance and monitoring of the Department's information systems to detect possible security breaches. However, CSMC could not demonstrate that it has full visibility to monitor all of the Department's systems for computer incidents. CSMC has a memorandum of agreement with the Office of the Secretary (OST) that calls for CSMC to enter into agreements with OAs that delineate the responsibilities for monitoring and managing OAs' networks and devices. CSMC did not provide copies of these agreements.

CSMC's lack of a comprehensive view and monitoring of all departmental networks and devices creates a risk that gaps in monitoring could expose DOT to security breaches.

Some OAs' Information System Administrators Have Not Disabled Inactive User Accounts

DOT's cybersecurity policy requires system administrators to close email and service accounts after 90 days of inactivity. Despite having complied in 2012 with a previous recommendation regarding proper closing of inactive accounts, the Department again has inactive accounts that it has not closed. We found over 7,000 user and service accounts that had passed 90 days of inactivity. Of these, 6457 were FAA consolidated network infrastructure accounts.

FAA reported that its method for disabling inactive user accounts, which is automated, was temporarily suspended to allow for network consolidation. Consequently, 6,457 FAA accounts were disabled until after more than 90 days of inactivity. FAA also reported that its new automation disables accounts after 60 days of inactivity but it will not be active until network consolidation is complete. User accounts that are inactive for long periods of time create a risk of access to information and information systems by individuals that are no longer authorized to access the systems.

Not all Department Computers Meet the Required Security Level for Use of Commercial Software

OMB requires agencies to adopt the U.S. Government Configuration Baseline (USGCB) settings for commercial software such as Windows. These system configurations provide the lowest acceptable level of security and ensure the efficient use of resources. To test DOT compliance, we selected a statistical sample of 756 devices out of 70,753 active computers. However, the OAs could not locate[14] 414 of the 756 devices sampled. Based on this sample, we estimate the OAs could not find or test 50.7 percent or 35,893 computers[15] in the universe of active computers during compliance scanning. Results from this year's scanning test represent about a 20 percent improvement from last year.

We tested the remaining 343 Windows computers in our statistical sample for USGCB settings. Based on our testing, we estimate that 85.4 percent of the approximately 34,860 available Windows computers in the Department's universe of computers met baseline settings.[16] This is a minor increase of 2.5 percent from 2013.

[14] We selected computers for testing from inventories that the OAs provided. However, the results of a scan of these 414 computers showed that they were not located on the network.

[15] Our estimate has a margin of error of +/-5.6 percentage points at the 90% confidence level.

[16] Our estimate has a margin of error of +/-7.9 percentage points at the 90% confidence level.

See table 4 for a summary of the Department's overall USGCB compliance for our sampled computers.

Table 4. Results of Sample Testing on USGCB for Windows Operating Systems

Component General Support Systems[a]	Computers Sampled	Controls Tested	Controls Passed	Controls Failed	Percent Passed[e]
COE[b]	68	18528	18024	504	97.3%
FAA LAN[c]	68	27762	22861	4901	82.3%
USMMA LAN	45	11790	11637	153	98.7%
Volpe Center LAN[d]	48	12321	9833	2488	79.8%
STB LAN	51	13311	11940	1371	89.7%
OIG Infrastructure	63	16443	16372	71	99.6%
Totals	**343**	**100155**	**90667**	**9488**	

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

[b] The Department's consolidated IT network infrastructure (email, desktop computing, network management, etc.).

[c] FAA's consolidated network infrastructure. On September 29, 2014, FAA provided the total number of workstations scanned and those that failed USGCB testing. We determined that FAA LAN has a 97 percent compliance rate for Windows 7/XP based on 9,222 compliant workstations out of 9,505 Windows 7/XP workstations scanned.

[d] Volpe reported that full compliance with USCGB settings is incompatible within a research and development/engineering environment, and noted that many of its workstations require special software for scientific and experimental purposes.

[e] Percent rounded.

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.

The Department Does Not Have a Complete 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, business process, and system. DOT's risk management program is not ready for implementation. Specifically, the program lacks a governance structure that meets NIST requirements.

The OAs reported that in the absence of a departmentwide program, they have developed their own programs. However, only FAA, FHWA, FRA, FTA, NHTSA, OIG, and PHMSA provided their internal risk management policies and procedures. FMCSA, MARAD, OST, OST-R, SLSDC and STB did not provide documented polices. Table 5 details the OAs' compliance with the risk management elements required by NIST.

Table 5. Risk Management Progress Summary

Risk Management Program Elements	**FAA**	**FHWA**	**FRA**	**FTA**	**NHTSA**	**OIG**	**PHMSA**
Internal policy documents risk management programs including descriptions of the roles and responsibilities of participants	N	Y	Y	Y	Y	Y	Y
Defined procedures to execute risk management programs	Y	Y	Y	Y	Y	Y	Y
Established comprehensive governance structures and follow organization wide risk management strategies	Y	Y	N	Y	Y	Y	Y
Established criteria for making risked based decisions	Y	Y	N	Y	Y	Y	Y
							Legend: N = No Y = Yes

Source: OIG analysis

The lack of a comprehensive 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 Implemented a Departmentwide Security Capital Planning Program

To ensure an adequate budget for security, OMB requires[17] agencies to plan for and track information security costs as part of their capital planning processes, and

[17] As part of its implementation of the Clinger-Cohen Act of 1996, formerly the Information Technology Management Reform Act, Public Law No. 104-106, codified at 40 U.S.C. § 11101, *et seq*. (2011).

to link these costs to their enterprise architectures (EA).[18] The Department has not implemented a departmentwide capital planning program for information system security. In October 2014, the Department issued its Information Technology Security Cost Estimating Guide, including budgeting responsibilities for IT security, and for estimating levels of effort and cost associated with implementing security controls. The OAs have until September 2015 to implement this guidance. In fiscal year 2014, in lieu of a standard methodology for estimating security costs, the OAs had the option to use their own estimating processes.[19] See table 6 for details on DOT's fiscal year 2014 IT security investments by OA.

[18] An EA defines an agency's mission, the information and technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. It includes both a baseline (current) and a target (planned) IT structure, and a plan for transitioning from the current to the planned.

[19] An organization's approach to the selection, management, and evaluation of IT security investments with use of the security model defined in an EA.

Table 6. Summary of DOT's Fiscal Year 2014 IT Security Investments

OA	Number of IT investments[a]	Total funding requested for IT security (in millions of dollars)[b.d]	Security cost estimation method established?
FAA	131	$34.6	N
FHWA	46	2.4	Y
FMCSA	21	1.9	N
FRA	20	0.3	Y
FTA	13	0.4	N
MARAD	20	0.7	N
NHTSA	20	0.1	Y
OIG	1	0.1	Y
OST	61	4.2	N
OST-R[c] (RITA/VOLPE)		1.4	N
PHMSA	14	0.1	Y
SLSDC	2	0.0	Y
STB	5	0.1	N
Total	**354**	**$46.3**	

Legend: N = No Y = Yes

[a] OMB Federal IT Dashboard fiscal year 2015 Edition Website (https://itdashboard.gov/portfolios) as of September 19, 2014.

[b] DOT's Oracle Primavera Portfolio Management (OPPM) system website as of September 9, 2014.

[c] OST established a new office—the Office of the Assistant Secretary for Research and Technology (RITA)—in January 2014. Its investments are included in OST's, but OPPM reports RITA's total separately.

[d] Dollar amounts rounded in millions.

Source: OIG analysis

The OAs have self-reported their security estimates but have not used estimation methodologies from which OST can base future projections. Furthermore, the reasonableness of their estimates is unknown. As a result of this lack of an implemented departmentwide methodology for estimating security funding, the Department cannot be sure that the OAs are efficiently and effectively planning and addressing security issues.

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

The Department's system-level controls are not sufficient to protect the systems' security and ensure that the systems can be recovered in the event of a serious breach. Persistent deficiencies impede DOT's efforts to comply with requirements to conduct ongoing security assessments, as required by DOT policy. In addition, we found deficiencies in (1) systems' authorizations to operate, (2) shared system security controls, (3) continuous monitoring of security controls, (4) oversight of contractor-operated systems, and (5) controls over identity and account management.

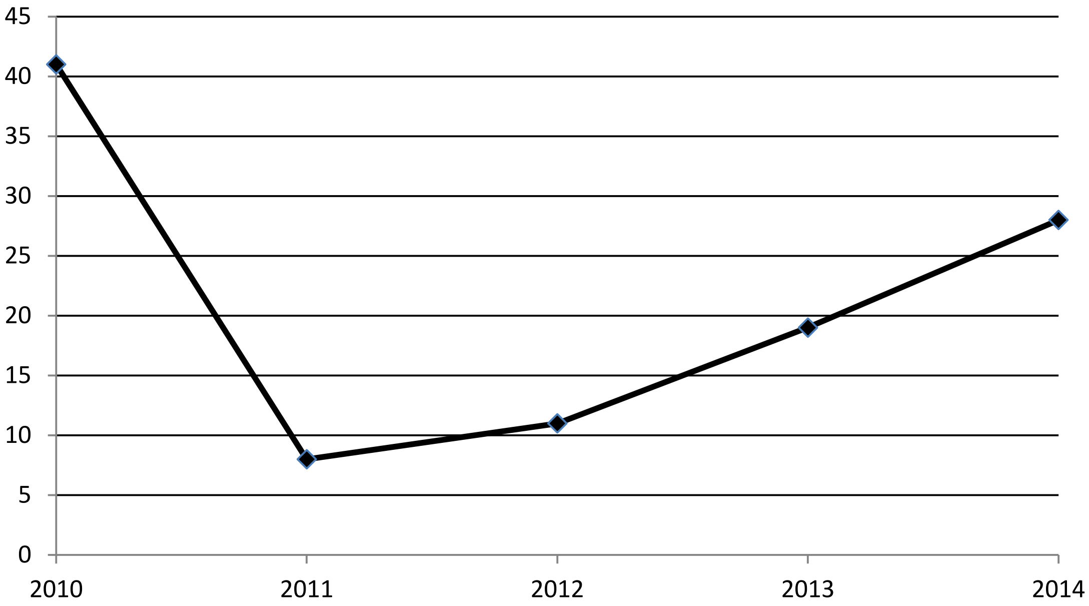
The OAs Have Not Implemented the Department's Risk Management Framework

OAs have not complied with NIST's risk management framework, as DOT policy requires. FISMA requires agencies to ensure information security is implemented in information systems to an acceptable level of risk. NIST's risk management framework provides guidance for agencies on security implementation. Specifically, the framework helps agencies ensure that they implement, assess, and monitor 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; continuous monitoring of security controls; use of personal identity verification cards for user access to systems and facilities; and contingency planning and testing.

OAs Lack Adequate Evidence that their Systems Are Ready To Be Authorized

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, we identified 28 systems whose authorizations to operate had expired. As shown in figure 1, these expired authorizations continue a trend of increasing numbers of unauthorized systems that started in 2012. Among the 28 systems, MARAD had 4 and FMCSA had 2 systems that have been unauthorized for 2 years. Four of RITA's systems had not been authorized for 3 years.

Figure 1. Expired Authorizations To Operate Over the Past 5 Years



Source: CSAM and OIG analysis

The system owners and information security system managers for these systems have not provided the authorizing officials with the required information for making risk based decisions for reauthorization. For example, we found POA&Ms that did not have updated information or complete annual security control testing. See table 7 for the list of expired authorizations to operate by OA.

Table 7. Systems Reported as Overdue for Reauthorization in 2014

OA	DOT System Reported as Outstanding for Reauthorization	No. of Systems by OA[a]
FAA	Office of Airports Local Area Network (ARP LANS)	3
	AST Local Area Network	
	Investment Planning and Management (IPM)	
FMCSA	CDLIS-Gateway	7
	CoTs DOT LAN	
	Electronic Document Management System	
	Enforcement Management Information System	
	Hazardous Material Package Inspection Program (HMPIP)	
	Licensing & Insurance	
	Performance & Registration Information Systems Management (PRISM)	
MARAD	BlackBoard	5
	Comprehensive Academic Management System (CAMS)	
	USMMA LAN	
	USMMA Student Information System	
	USMMA Distance Learning Management System for Graduate Program	
NHTSA	PRISM	5
	NHTSA Inventory System	
	Crash Test Database	
	Traffic Records Improvement Program Reporting System	
	WEB System	
OST	Case Tracking System (CTS)	3
	Image Management System	
	Rulemaking Management System (RMS)	
OST-R (RITA)	RITA Mission Support	4
	RITA Web	
	Transtats	
	TSI Infrastructure	
STB	Local Area Network	1
	TOTAL	**28**

Source: CSAM and OIG analysis

Furthermore, as shown in table 8, 4 of 20 sample systems had incomplete authorization documentation.

Table 8. Sample Systems' Security Authorizations and Control Testing

OA	Systems Tested	Systems Without Adequate Security Authorization
FAA	10	1
FHWA	2	
FMCSA	1	
FRA	1	
FTA	1	
MARAD	1	1
NHTSA	1	1
OIG	0	
OST	1	
PHMSA	1	
RITA	1	1
SLSDC	0	
STB	0	
Total	20	4

Source: OIG analysis

The OAs completed baseline security control testing for these 20 sample systems' first security authorizations, but did not provide evidence that they had established plans for continuous system monitoring—required by both NIST and departmental policy.

DOT Lacks Effective Procedures for Monitoring Common Security Controls

NIST requires providers of common controls—security controls that support multiple information systems—(1) have policies and procedures for their use, (2) to document the controls in separate security plans, (3) conduct ongoing assessment of the common controls' security, monitor their effectiveness, and (4) inform users when changes occur that may adversely affect the protections provided by or expected of these controls.

The Department has not finalized procedures and oversight pertaining to common controls. The COE is still conducting planning and research to determine the resources needed to ensure that common controls are properly used, implemented, and monitored. Furthermore, FAA's Air Traffic Organization has not completed development of definitions and processes to support risk assessments of common controls. FAA reported that it is developing standards for use of common controls but did not provide a scheduled implementation date.

In addition, for these 20 sample systems, the OAs had no agreements between the system owners and common control providers. These agreements establish the parties' responsibilities, accountabilities and security requirements. The owners of these 20 systems allowed their systems to begin functioning with the use of common controls without executing these agreements.

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

DOT's Continuous Monitoring of Security Controls Remains Insufficient

Continuous monitoring provides ongoing awareness of information security, vulnerabilities, and system threats. NIST's guidance calls for agencies to implement programs to continuously monitor security controls. OMB requires agencies develop a continuous monitoring strategy to help identify what the agencies need to do in order to respond to cyber threats. DOT has not executed all elements of an effective continuous monitoring program. See Table 9 for the required elements of a continuous monitoring program and which OAs have implemented them.

Table 9. Elements of a Continuous Monitoring Program

OA	Policy	Architecture[a]	Metrics	Monitoring/ Assessment Frequencies	Status Reporting
FAA	Y	N	N	N	N
FHWA	Y	N	N	N	N
FMCSA	Y	N	N	N	N
FRA	Y	N	N	N	N
FTA	Y	N	N	N	N
MARAD	Y	N	N	N	N
NHTSA	Y	N	Y	N	Y
OIG	Y	N	Y	N	Y
OST	Y	N	N	N	N
PHMSA	Y	N	N	N	N
OST-R (RITA/VOLPE)[a]	N	N	N	N	N
SLSDC	N	N	N	N	N
STB	N	N	N	N	N

[a] OST-R is organizationally reported as both RITA and VOLPE. RITA did not provide any continuous monitoring plan information. Volpe did provide a plan.

Source: OIG analysis

In 2012, OCIO initiated an automated enterprise continuous monitoring program (AECM) for departmentwide information security continuous monitoring. However, we found that OCIO does not have comprehensive guidance for the OAs to implement AECM and use it for the identification and mitigation of security weaknesses. Furthermore, the OCIO has not clearly defined how frequently they should collect data for effective monitoring and decision-making for mitigation, such as which weaknesses to prioritize.

The lack of an effective continuous monitoring program that includes a set of integrated tools to automate the collection and analysis of data on the system's security makes it difficult for both the Department and OAs to make effective risk-based decisions.

DOT Has Made Progress in PIV Access Implementation but Completion Dates are Uncertain

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. However, DOT still has not implemented the use of PIV cards for all of its employees and contractors, which total 70,277.

PIV implementation has been a persistent problem at DOT. Documentation provided to OIG during this audit shows that in fiscal year 2013, 83 Department personnel were using PIV cards for network access. Towards the end of fiscal year 2013, OCIO began aggressive efforts to improve compliance with OMB's requirements for PIV card use for network access, including increased coordination with the OAs and monitoring of their progress. OCIO also instituted a PIV waiver process to allow OAs to request extensions for issuance of PIV cards. For example, FAA requested waivers for employees who fall under union agreements to allow additional time to coordinate with unions. OCIO has granted waivers for PIV access to networks to 27,851 of 70,277 unprivileged users[20] (39.6 percent). The majority of these waivers have gone to personnel in FAA's Air Traffic Organization. OMB allows exceptions to the use of PIV credentials due to extenuating circumstances, such as for systems that are being decommissioned. OCIO's use of a waiver process illustrates the difficulties the Department continues to have in establishing PIV use for system access for approximately 40 percent of its unprivileged users.

In its September 2014 report to OMB regarding the transition to PIV access, OCIO reported that 42,426 of 70,277 unprivileged accounts require PIV card access to networks, and that 10,123 actually use PIV cards for access, or 23.8 percent of the total number of users required to use PIV cards. However, OCIO arrived at these figures by subtracting 27,851 unprivileged users that have been waived from the requirement from the Department's 70,277 total personnel. By doing so, DOT's results do not illustrate the risks assumed by the large amount of users covered by waivers. Based on the total population of unprivileged users who need PIV access, only 14.4 percent of the Department's personnel currently have PIV access to departmental networks. See table 10 for a summary. The Department also reported that 10 percent of its users with privileged access are required to access departmental networks with PIV cards, but provided no supporting evidence. Notably, FHWA, FTA, NHTSA, OST, RITA, Volpe, and SLSDC exceeded the Administration's goal for fiscal year 2014 of 75 percent of the personnel required to have PIV access actually having it, even without including waivers in their calculations.

[20] An unprivileged user utilizes an account for everyday access to applications such as email and data processing. A privileged user is authorized and trusted to perform security-relevant functions that ordinary, or unprivileged, users are not authorized to perform.

Table 10: Summary of DOT's Unprivileged User Access to Networks

OA	Total Unprivileged Users that require PIV access	Unprivileged Users with Approved Waivers for PIV access	Unprivileged Users without waivers for PIV access	Unprivileged Users with Activated PIV Access	Unprivileged Users without Activated PIV Access	% of Unprivileged Users with Activated PIV Access Minus Waived Users	% of Total Unprivileged Users without Activated PIV Access
FAA	57,761	24,445	33,316	1,050	32,266	3.2%	1.8%
FHWA	3,764	467	3,297	3,297	0	100.0%	87.6%
FMCSA	1,336	1,072	264	264	0	100.0%	19.8%
FRA	1,006	641	365	365	0[b]	102.5%	36.3%
FTA	706	3	703	703	0	100.0%	99.6%
MARAD	918	392	526	526	0	100.0%	57.3%
NHTSA	1,052	150	902	902	0	100.0%	85.7%
OIG	431	132	299	253	46	84.6%	58.7%
OST[a]	1,259	59	1,200	1,200	0	100.0%	95.3%
− RITA	140	0	140	140	0	100.0%	100.0%
− TSI	49	27	22	22	0	100.0%	44.9%
− VOLPE	982	0	982	982	0	100.0%	100.0%
PHMSA	603	325	278	278	0	100.0%	46.1%
SLSDC	133	1	132	132	0	100.0%	99.2%
STB	137	137	0	0	0	0.0%	0.0%
Totals	**70,277**	**27,851**	**42,426**	**10,114**	**32,312**	**23.8%**	**14.4%**

[a] OST is the total sum of RITA, TSI, and VOLPE individual totals.

[b] Amended to correct error reporting of -9 in OCIO data.

Source: OCIO's September 2014 report on departmental PIV access

OCIO also reported that only 90 of 445 applications[21] on the Department's network are enabled to allow access with PIV cards, and did not provide a plan for enabling the remaining systems with the exception of FAA. Approximately 81 of FAA's 303 applications are PIV card enabled. FAA has set a goal to have the remaining 222 systems PIV enabled by end of fiscal year 2015.[22]

Moreover, during an audit of FTA's financial system applications, OIG's contractor found that FTA had not established PIV access for its financial systems.[23] The risks of unauthorized and undetected access to these systems resulted in a material weakness in the department's financial statements.

Furthermore, OST, which is responsible for facilities security and access, did not provide updated plans for enabling DOT facilities for PIV access. FAA reported that it has started upgrading its facilities to accept PIV cards for access and anticipates completing the transition by the end of fiscal year 2018. However, FAA did not provide a plan with milestones and completion dates.

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 Contingency Planning Program Lacks Oversight

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

We evaluated 20 sample systems, and found that four OAs had deficiencies in contingency planning and testing for at least one system. See table 11 for a summary of deficiencies in the sample systems.

[21] As of April 14, 2014, the Department reported a baseline population 445 applications.

[22] However, OCIO stated to us that it questioned FAA's ability to complete the conversion of its remaining systems by 2015.

[23] We will provide further detail on this finding and related recommendations in our upcoming report on the fiscal year 2014 DOT financial statement audit.

Table 11. Summary of DOT's Sample Systems with Deficiencies in Contingency Planning and Testing

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

Legend: N = No Y = Yes

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. As a result, a disruption may result in information or systems not being available to accomplish DOT's mission.

The Inventory in CSAM of FAA's Contractor-Operated Systems Is Incomplete

OMB requires agencies to maintain up-to-date inventories of their information systems. These inventories must designate each system as either organization operated or contractor operated, based on who manages the system—the agency or an outside entity. Contractor operated systems are those that are either fully or partially owned or operated by a contractor, another agency, or other entity.

Based on the guidance for categorizing systems,[24] the OAs have recategorized 22 of the systems identified in 2013 as incorrectly designated as OA-operated. However, FAA had miscategorized 97 systems and has corrected only 11, leaving 86 systems incorrectly categorized as organization operated. FAA informed us that the 86 should not be classified as contractor systems, and does not have plans to update the contractor classification in CSAM. FAA did not provide a justification for not recategorizing these systems.

[24] DOT FISMA Inventory Guide, June 2012.

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

OAs that Use Cloud Computing Still Have Not Complied With Requirements

Cloud computing enables convenient access to shared pools of computing resources, such as networks, servers, storage, and applications, that can be rapidly provisioned and released with minimal management effort. Cloud computing resources are either private—exclusive use by an organization—or public—the cloud infrastructure is open for use by 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 templates help agencies satisfy FedRAMP's requirements with standard language for contracts and service agreements with their providers.

Similar to last year, we found that 6 OAs—FHWA, FAA, FRA, OST, NHTSA, and FMCSA—using cloud computing could not provide evidence of their compliance with this requirement. We also found that the Department does not maintain a reliable inventory of cloud based systems. It also has not reviewed existing cloud computing agreements to assess compliance with departmental policy, including security requirements.[25] 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.

THE DEPARTMENT LACKS ADEQUATE REMEDIATION PLANS FOR SYSTEM WEAKNESSES

FISMA requires that agencies develop processes to remediate security weaknesses. OMB requires departments to develop POA&Ms for identified 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 risk criteria. The policy also requires

[25] We will provide further detail on these findings and recommendations in our upcoming report on the Department's cloud computing program.

OAs to record their POA&Ms in CSAM. However, DOT’s POA&Ms are still not managed in accordance with Federal and departmental requirements. OAs have 5,628 open POA&Ms—a reduction of only 1,086 (16 percent) from 2013—some of which date from 2009. We also found:

- 1186 POA&Ms did not identify planned start dates. OAs must include dates they plan to begin remediation of each weakness.
- 2935 POA&Ms—149 high priority and 967 moderate priority—had no documented remediation costs.
- 131 POA&Ms—23 high, 69 moderate, and 39 low priority—had only $1 listed as remediation cost. The Department has not yet implemented policy and procedures for OAs to determine actual security cost estimates. DOT IT Security Cost Estimation guide target date for implementation is September 2015.

See table 12 for specific details on the issues we identified regarding POA&Ms.

Table 12. Summary of POA&Ms Opened between 2009 and 2014 without Planned Start Dates or Documented Remediation Costs

OA	Total Open POA&Ms	With Planned Start Date mark as "TBD"	No Documented Cost
FAA	3218	8	1722
FHWA	0	0	0
FMCSA	639	338	607
FRA	149	22	62
FTA	241	0	0
MARAD	790	702	207
NHTSA	8	6	6
OIG	3	0	0
OST[a]	326	2	107
OST-R (RITA)	189	108	189
PHMSA	16	0	0
SLSDC	1	0	0
STB	48	0	35
Total	**5,628**	**1186**	**2935**

[a] Includes the COE's 55 POA&Ms

Source: POA&Ms in CSAM as of July 31, 2014

We also identified two other noncompliance issues related to the remediation of security weaknesses:

1. In the information provided to authorizing officials for reauthorization of 4 of the systems in our sample of 20 systems, the OAs did not include information on all identified security weaknesses in CSAM.

2. A 2010 OCIO-commissioned assessment of the COE's security did not include review and remediation plans for COE weaknesses listed in CSAM. Additionally, OCIO did not provide evidence that it has addressed these weaknesses.

In addition, OCIO did not provide quarterly or monthly compliance review reports on the OAs' adherence to the Department's security policy. In April 2014, the CIO required the Department's information system security managers to take action on 114 POAMs designated as high priority. Because OCIO did not provide compliance review reports, we could not determine whether these weaknesses were remediated. Unresolved POA&Ms make it difficult for DOT to ensure systems are secured and protected.

CONCLUSION

While DOT has improved some of its security controls, weaknesses remain that could affect the confidentiality, integrity, and availability of departmental data and systems. Access control inadequacies such as identification and authentication, audit and monitoring, and physical security, and weaknesses—including network monitoring, configuration management, system authorization, and continuity of operations—continue to put DOT's systems and data 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 22 recommendations that are still open from prior FISMA reports.

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 SP800-53A 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 and improve tracking. 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, and 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 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.

13. Develop a plan to periodically review waived accounts to determine if they should be transitioned to PIV required status. Create a POA&M with a planned completion date to monitor and track progress.

14. Work with components to revise their plans to effectively transition the remaining users to require privileged 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.

AGENCY COMMENTS AND OIG RESPONSE

We provided a draft of this report to the Department on November 3, 2014 and received its response on November 12, 2014, which can be found in its entirety in the appendix to this report. In its response, the Department states that it has improved its information security posture but recognizes that more work is required. The office plans to provide to us, by January 31, 2015, specific responses to each recommendation that identify and prioritize planned actions and anticipated milestones. However, until we receive the Department's complete response including specific planned actions and anticipated milestones, we consider all recommendations open and unresolved.

The Department also notes in its response that it is troubled by our reference in the report to the fire at a Chicago air traffic facility. It states that "this matter is still under investigation and nothing at this time indicates that there was a weakness in its information security system that contributed to this unfortunate incident." However, the Department must recognize that the incident resulted in the cancellations of hundreds of flights and underscores the need for effective contingency plans. As noted in our report, we are conducting an audit to assess the contingency plans and security protocols at the Chicago Air Traffic Facility.

ACTIONS REQUIRED

Upon receipt of OCIO's January 31, 2015 submission, as stated above, we will determine whether the Office's specific planned actions and anticipated milestones satisfy the intent of each recommendation. Based upon this review, we will determine the status and resolution of each recommendation. All corrective actions are subject to the follow-up provisions in DOT Order 8000.1C.

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

FISMA requires us to perform annual independent evaluations to determine the effectiveness of the Department'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, we assessed a subset of 20 of 458 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 13 for sampled systems and Table 19 for DOT system inventory). Of the systems selected for review, 18 were available but one was retired and one was removed from operational status. To replace these systems, we selected two substitute systems for review. Our random selection was based on a universe of 246 moderate and high systems that we never reviewed before. To evaluate USGCB compliance, we selected a statistical sample of 756 of 70,753 devices to scan for compliance. We created a script to extract the test results of USGCB controls from 343 of 756 devices that were available for scanning.

We evaluated prior year recommendations and supporting evidence to determine what progress had been made in the following areas: continuous monitoring; configuration management; 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; security capital planning; and account and identity management. Our tests included analyses of data contained in the Department's CSAM system, 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 also reviewed the Department's progress in resolution of weaknesses and implementation of recommendations identified in our prior FISMA reports.

Per agreement with the Department, our request for supporting documentation was due July 31, 2014. We performed our information security review work between February 2014 and November 2014. We conducted our work at departmental and OA Headquarters' offices in Washington, D.C.

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.

Table 13. OIG's Representative Subset of DOT Systems, by OA

	System	Impact Level[a]	Contractor System?[b]
	Federal Aviation Administration		
1	FAA - Print Request Information Tracking (PRINT)	Moderate	N
2	OGE-450 (Eastern Region Office of Government Ethics-450)	Moderate	N
3	ATO SCI (Air Traffic Organization Superior Contribution Increase)	Moderate	N
4	FOIA NTS	Moderate	N
5	Aviation Environmental Design Tool	Moderate	N
6	CATS (ARP) (Certification Activity Tracking System)	Moderate	N
7	ITS (Investigative Tracking System)	Moderate	N
8	OFDPS (Off Shore Data Processing Station)	Moderate	N
9	AIE (Accident Incident Enforcement)	Moderate	N
10	MSS (Medical Support Systems)	High	N
	Federal Highway Administration		
11	Fiscal Management Information System (FMIS)	High	Y
12	Western Federal Lands General Support System	Moderate	Y
	Federal Motor Carrier Safety Administration		
13	FMCSA Portal	Moderate	N
	Federal Railroad Administration		
14	FRA - PRISM	Moderate	Y

	System	Impact Level[a]	Contractor System?[b]
	Federal Transit Administration		
15	FTA - PRISM	Moderate	Y
	Maritime Administration		
16	Ship Manager Performance Evaluation and Appraisal System	Moderate	Y
	National Highway Traffic Safety Administration		
17	FARS	Moderate	Y
	Office of the Secretary of Transportation		
18	Grants Notification System (GNS)	Moderate	Y
	Pipelines and Hazardous Materials Safety Administration		
19	Safety Monitoring and Reporting Tool	Moderate	Y
	Research and Innovative Technology Administration		
20	Volpe Center GSS/LAN	Moderate	Y

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.

[b] DOT's definition of contractor system.

Source: OIG

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

- *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.
- *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 B. Status of Previous Years' Recommendations

Table 14. Status of OIG's Recommendations for Fiscal Year 2013

No.	Status	Recommendation
1	Open	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	Open	Increase oversight of OA's 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.
3	Open	In conjunction with FAA's CIO, institute periodic scanning for USGCB and baseline compliance for the FAA LANs to include analysis of results to remediate deficiencies. Create a POA&M to track progress and verify completion of the action.
4	Open	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	Open	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	Open	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	Open	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	Open	Obtain and review existing cloud computing agreements to assess compliance with agency policy, including security requirements. Report exceptions to OA management.

Table 15. Status of OIG's Recommendations for Fiscal Year 2012

No.	Status	Recommendation
1	Open	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.
2	Closed	Establish timeframes for incident remediation based on risk.
3	Open	Remove inactive computer devices from the Active Directory databases by (a) requiring the OAs to develop a POA&M to address the removal of such devices in a timely manner, (b) reviewing the adequacy of the POA&Ms, and (c) monitoring the OA's clean-up process through completion.
4	Open	Develop, document and approve an enterprise-wide risk management program and strategy as defined by NIST 800-39.
5	Open	Identify and work with common control providers to develop and implement a security plan that will ensure that systems that inherit common controls are adequately protected and C&A'd.

Table 16. Status of OIG's Recommendations for Fiscal Year 2011

No.	Status	Recommendation
1	Partially Closed	Address these policy and procedural weaknesses: • ssue 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.
3	Open	In conjunction with OA CIOs, establish incident monitoring and detection capabilities to include all of the Department's systems and facilitate central and real-time reporting.
4	Open	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.
5	Closed	In conjunction with OA CIOs, verify that backup media are properly secured and regularly tested.
6	Open	In conjunction with OA CIOs, verify that minimum security controls are adequately tested for deficient systems.

Table 17. Status of OIG's Recommendations for Fiscal Year 2010

No.	Status	Recommendation
1	Closed	Address these policy and procedural weaknesses: • Develop procedural guidance for the C&A process. In addition, modify existing certification and accreditation policy and procedures to address inheritance of common information security controls, and to provide procedural guidance to modes. • Correct POA&M policy to prioritize weaknesses in a way that ensures that high priority weaknesses are resolved before medium priorities, and medium ones before low ones. In addition, develop procedural guidance to ensure consistency of the POA&M process and to facilitate CIO's oversight and management of weaknesses. • In conjunction with the modes, develop procedural guidance for tracking and training personnel with significant security responsibilities. This guidance should address maintaining complete inventories of such personnel, and the training needed and provided. • Enhance high-level policy with procedural guidance to ensure consistency of the network accounts and identity management. • In conjunction with the Assistant Secretary for Administration, complete departmentwide PIV operating procedures, including procedures to terminate PIV cards. • Review and revise all configuration management policy and develop specific details for activities that are common across the department. As part of this effort, develop procedural guidance that would define requirements for OAs to use when developing configuration management procedures specific to their operation. • Develop procedural guidance that would define requirements for OAs to use when developing incident handling procedures specific to their operation. • Enhance policy and procedural guidance to incorporate detailed guidance for managing, monitoring and reporting FDCC compliance, including the use of SCAP tools to ensure FDCC compliance. Once policy adequately addresses contractor oversight per Recommendation 4 of last year's report, develop relevant procedural guidance. This policy should establish the criteria and guidelines for DOT's identification and reporting of contractor systems consistent with OMB requirements. • Enhance high-level policy with procedural guidance to ensure remote access and wireless networking is authorized, managed and monitored in compliance with OMB, NIST and DOT policies.
2	Closed	To the extent the OAs require their own guidance, review guidance to verify compliance with department policies and procedures.
3	Closed	Implement a quality assurance process to review OA specific configuration management procedures to ensure that they adhere to the departmental policy and Federal requirements.
4	Closed	Implement a process to review OAs security configuration management practices and software scanning capabilities. Provide monitoring of OAs practices to ensure they are adhering to the policy and practices.
5	Closed	Require OST to implement required system patches on their Delphi system.

No.	Status	Recommendation
6	Closed	Conduct scanning of all DOT networks to ensure compliance with FDCC requirements. In addition, review results of modal SCAP compliance scans to identify and resolve incorrect FDCC settings.
7	Closed	Require and approve deviation requests for those non-conforming settings that are truly needed and for which risks have been mitigated and accepted.
8	Closed	Conduct periodic tests to assess FDCC compliance and deployment of patches, including service packs.
9	Closed	Analyze the incorrect FDCC configuration settings identified in our testing, and for those that do not have approved deviations, require OAs to create POA&Ms to correct the settings.
10	Closed	Implement a practice to review OA specific incident handling procedures to ensure that they adhere to the departmental policy.
11	Closed	Implement a process to review reported incidents to ensure timely reporting to US-CERT. In addition, provide monitoring of incidents reported to ensure all required data in the tracking system(s) is up-to-date for incidents sent and data received back for US-CERT.
12	Closed	Review FHWA, FMCSA, FRA, FTA and RITA automated scans confirming timely resolution of vulnerabilities. If deficiency is found require OA to provide corrective action and to update plan of actions and milestone to address weakness.
13	Closed	Require OAs to reconcile their contractor records with DOT security department and update their records accordingly. Monitor and report to the Deputy Secretary, Operating Administrations' progress in resolving the discrepancy with their contractor records and DOT security department.
14	Open	Identify and implement automated tools to better track contractors and training requirements.
15	Closed	In conjunction with the MARAD, create a POAM for each system that is missing a certification and accreditation. This POAM should be properly prioritized to ensure this critical matter is immediately addressed.
16	Closed	In conjunction with MARAD, promptly update Cybersecurity Assessment and Management (CSAM) system to reflect its current system inventory and related information (including status of certification and accreditation).
17	Closed	Work with MARAD to finalize agreements with C&A service providers to certify MARAD systems.
18	Open	Review the results of OA assessments to determine an accurate inventory of contractor systems.
19	Closed	Work with the Department's acquisition personnel to develop common contract language that requires IT contractors to enforce applicable FISMA and OMB requirements. Once this language is approved, review all new planned IT acquisitions, prior to award, to verify that this clause is contained in the statement of work or comparable document.
20	Closed	Research and standardize automated tools that will proactively monitor remote devices connecting to DOT networks.
21	Closed	Conduct tests of remote access solutions to ensure they comply with Federal requirements and DOT guidance.

No.	Status	Recommendation
22	Closed	In conjunction with the Assistant Secretary for Administration, develop a Departmentwide implementation plan that specifies resources needed, responsible parties, strategies for risk mitigation, etc., to ensure that all employees and contractors receive PIV cards by December 31, 2010.
23	Open	Implement the use of PIV cards as the primary authentication mechanism to support multi-factor authentication at the system and application level for all DOT's employees and contractors.
24	Closed	Perform periodic reviews of active user accounts and network devices to identify accounts that need to be disabled.
25	Closed	Work with OAs to identify and logically segregate user accounts and service (role) accounts.
26	Closed	Work with OAs to implement automated mechanisms to disable inactive accounts, as specified by DOT policies, and to audit account creation, modification, disabling, and termination actions.
27	Closed	Educate and assist OAs in implementing dual accounts for administrators. Subsequently, conduct reviews to determine that all DOT GSSs use these accounts.

Source: OIG

Table 18. Status of OIG's Recommendations for Fiscal Year 2009

No.	Status	Recommendation
1	Closed	Revise the incident response policy to identify conditions under which incidents should be reported to law enforcement (i.e., OIG), how the reporting should be performed, what evidence should be collected, and how it should be collected.
2	Closed	Revise the security awareness and training policy to include the identification of all users, such as employees, contractors, and others requiring access to DOT information systems. Include provisions in the policy to separate these active user accounts from the non-person accounts.
3	Closed	Revise training policy to list the job functions that require specialized security training and the type of specialized training that is required for those job functions as described in NIST SP 800-16.
4	Closed	Revise policy to address security of information and information systems managed by contractors, including information security roles and responsibilities, security control baselines and rules for departures from baseline, and rules of behavior for contractors and minimum repercussions for noncompliance.
5	Closed	Revise the interface agreement policy to incorporate necessary elements, such as purpose of the interconnection, description of security controls, schematic of interconnection, timelines for terminating or reauthorizing the interconnection, and authority of establishing the interconnection.
6	Closed	Revise the plan of action and milestones policy to address all the OMB requirements, including description of weakness, scheduled completion date, key milestones, changes to milestones, source of the weakness, and status.
7	Closed	Ensure that the Federal Aviation Administration, Saint Lawrence Seaway Development Corporation, and Pipeline and Hazardous Materials Safety Administration have deployed DOT approved configuration baselines and tools to assess implementation status**.**
8	Closed	Use automated tools to periodically verify status of completion reported by Operating Administrations and identify deviations from the approved baseline configurations.
9	Closed	Require Operating Administrations to manage identified deviations from approved baseline configurations by tracking and resolving significant baseline configuration weaknesses in plan of actions and milestones.
10	Closed	Work with Operating Administration Chief Information Officers to ensure that all new IT contracts include the acquisition language on common security configurations as required by DOT and OMB M-07-18.
11	Closed	Work with the CSMC to develop a process to ensure that all Department of Homeland Security reference numbers are received and entered into the DOT tracking system for confirmation.
12	Closed	Develop and establish a tracking system that effectively and routinely accounts for all active contractors requiring security awareness training.
13	Closed	Develop a mechanism to enforce that all employees including contractors with login privileges have completed the required annual security awareness training in order to gain and maintain access to Department information systems.
14	Closed	Identify and ensure all employees with significant security responsibilities take the necessary specialized security training to fulfill their responsibilities.

No.	Status	Recommendation
15	Closed	Monitor, and report to the Deputy Secretary, Operating Administrations' progress in resolving long overdue security weaknesses, reestablishing target completion dates in accordance with departmental policy, providing cost estimation for fixing security weaknesses, prioritizing weaknesses, and recording all identified security weaknesses in plan of actions and milestones.
16	Open	Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.
17	Closed	Require Chief Information Security Officer and Operating Administrations conduct a review to identify all interfaces with systems external to the Department, ensure related security agreements are adequate, and track them in the Cybersecurity Assessment and Management system.
18	Closed	Ensure that Maritime Administration properly inventories its information systems and tracks them in the Cybersecurity Assessment and Management system. (MARAD)
19	Closed	Ensure that Maritime Administration certifies and accredits each system in the revised inventory. (MARAD)
20	Open	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.
21	Closed[a]	Require Federal Aviation Administration, Federal Highway Administration, Federal Railroad Administration, Maritime Administration, Office of the Secretary of Transportation and Pipelines and Hazardous Materials Safety Administration to conduct system contingency testing of the systems that did not have evidence that of such tests.
22	Closed	Develop a process to ensure Operating Administrations continuously monitor and test information system security controls.
23	Closed	Finalize the inventory count for systems containing privacy information.
24	Closed	Work with Operating Administrations to complete privacy impact assessments for applicable information systems.
25	Closed	Work with the Federal Aviation Administration to establish a reasonable target date for the completion of the reduction of social security numbers recorded in its systems.
26	Closed[b]	Implement 2-factor authentication for remote access.
27	Closed	Implement NIST-approved encryption on all mobile computers/devices.

[a] Replaced with 2011 Recommendation No. 3.

[b] Merged into 2010 Recommendation No. 23.

Source: OIG

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

Table 19. System Inventory Counts for Fiscal Years 2013 and 2014

Organization[a]	**FY 2013**	**FY 2014**
Common Operating Environment (COE)	1	1
Federal Aviation Administration (FAA)	303	320
Federal Highway Administration (FHWA)	21	20
Federal Motor Carrier Safety Administration (FMCSA)	18	16
Federal Railroad Administration (FRA)	15	12
Federal Transit Administration (FTA)	6	6
Maritime Administration (MARAD)	22	19
National Highway Traffic Safety Administration NHTSA)	10	10
Office of Inspector General (OIG)	3	2
Office of the Secretary (OST)	29	26
Pipeline and Hazardous Materials Safety Administration (PHMSA)	7	7
Research and Innovative Technology Administration (OST-R)\VOLPE[b]	17	17
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)[c]	1	1
Total Systems	**454**	**458**

[a] For purposes of reporting under FISMA, we consider "Operating Administrations" to include all organizations listed above.

[b] For the purpose of reporting systems inventory, RITA (OST-R) and Volpe are totaled together.

[c] 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 the Department of Transportation. Per Memorandum of Understanding (MOU) dated September 2013 between DOT and COE, the STB is expected to operate in accordance with federal and DOT policies to ensure the overall security and integrity of both the STB and COE network.

Source: CSAM as of August 1, 2014 and OIG analysis

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Nathan Custer	Program Director
Michael Marshlick	Project Manager
Martha Morrobel	Information Technology Specialist
Tracy Colligan	Information Technology Specialist
Jenelle Morris	Information Technology Specialist
Jo’Shena Jamison	Information Technology Specialist
Antione Searcy	Information Technology Specialist
Gary Fishbein	Referencer
Allison La Vay	Referencer
Petra Swartzlander	Senior Statistician
Megha P. Joshipura	Statistician
Karen Sloan	Communication Officer
Susan Neill	Writer-Editor
Christina Lee	Graphics Specialist

Exhibit D. Major Contributors to This Report

APPENDIX. AGENCY COMMENTS

Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Subject: **ACTION**: Management Response to the Office of Inspector General (OIG) Draft Report on Federal Information Security Management Act 2014

Date: NOV 12 2014

From: Richard McKinney
DOT Chief Information Officer

Reply To
Attn. Of:

To: Calvin L. Scovel III
Inspector General

Information security is a priority for the Department of Transportation (DOT). The Office of Inspector General's (OIG) 2014 Draft Report on the Federal Information Security Management Act recognizes the significant progress that DOT has made to increase network traffic consolidation through trusted internet connection (TICs), increase deployment of personal identity verification cards, and improve compliance with configuration standards. Although we have improved our information security posture over the past year, we recognize that more work is required, and our efforts must continue to evolve with ever-changing cybersecurity challenges. Consistently working with the Operating Administrations (OA), the Office of the Chief Information Officer (OCIO) provides comprehensive guidance, updates controls, assesses risk, and provides oversight. These efforts allow the Department to maintain critical operational systems and to be responsive to new requirements.

We remain troubled with the report's reference to the fire at a Chicago air traffic facility. This matter is still under investigation and nothing at this time indicates that there was a weakness in its information security system that contributed to this unfortunate incident. Leaving this sentence in the report is misleading and raises unnecessary concerns to the travelling public.

With respect to our efforts on a few areas where OIG provided findings, we offer the following comments:

- The report identifies several deficiencies stating that DOT has failed to meet FISMA, OMB, and NIST requirements in the areas of configuration standards, PIV card implementation, and security authorization. DOT notes that NIST guidance[26] allows for deviations to the extent there is a risk assessment and the business owner accepts the risks. In each of these areas, DOT has conducted a risk assessment and determined to accept the risk.

- The report sets forth expectations and identifies deficiencies in the area of continuous monitoring. However, it fails to recognize that the steps DOT should take are dependent upon actions outside of its control that must be taken by other external organizations.

- The report includes findings related to DOT guidance and architecture associated with DOT's continuous monitoring program. The DOT OCIO already has established an enterprise-wide strategy for Information Security Continuous Monitoring (ISCM) -- which includes Continuous Diagnostics and Monitoring (CDM) -- and we are fully engaged in the Department of Homeland Security's (DHS) CDM initiative. DOT is participating in the first phase of DHS's CDM program, and our processes will be updated after DOT's CDM solution has been awarded, and our post-award activities have begun. The DOT OCIO plans to leverage DOT's existing guidance (the Department's Security Authorization and Continuous Monitoring Guide), and to apply available resources to develop policy and guidance updates in other areas until such time as the awards on the DHS CDM have been made, products are selected, and integration activities have begun. Additionally, 75% of DOT Components have begun implementation of Component-level continuous monitoring strategies and programs.

- With respect to DOT's risk management and governance process, the OCIO agrees that there are opportunities for improvement in this area. Security risk management is one element in the overall risk management process, and should be integrated into the existing DOT governance structure and program. To this end, DOT finalized a security cost estimation guide that supplements the existing DOT Integrated Program Planning and Management Framework.

- The report notes the progress we have made in the deployment of Personal Identity Verification (PIV) cards, but we wish to further emphasize our progress in this effort. Since June 2013, DOT progressed from approximately 0% to over 30% required use of PIV cards.

We intend to provide, by January 31, 2015, a specific response to each recommendation that identifies and prioritizes actions planned and anticipated milestones, where appropriate. As we move forward, we will prioritize these matters, based on the OIG's work and recommendations, government-wide priorities, dot strategic initiatives, available resources, and data available from the department's own monitoring and risk management systems. 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. Please contact me with any questions.

[26] NIST SP 800-37, SP 800-39, SP 800-137.