Office of Inspector General

Audit Report

FISMA 2013: DOT HAS MADE PROGRESS, BUT ITS SYSTEMS REMAIN VULNERABLE TO SIGNIFICANT SECURITY THREATS

Department of Transportation

Report Number: FI-2014-006
Date Issued: - November 22, 2013

Memorandum

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

Subject: **ACTION:** FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats
Report Number: - FI-2014-006

Date: November 22, 2013

From: Calvin L. Scovel III
Inspector General

Reply to Attn. of: JA-20

To: Chief Information Officer

The Department of Transportation's (DOT) operations rely on more than 450 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 and disburse approximately $90 billion in Federal funds annually.

To protect Federal IT systems, the Federal Information Security Management Act (FISMA) of 2002 requires agencies to develop, document, and implement Departmentwide information security programs. FISMA also requires agency program officials, chief information officers (CIO), and inspectors general to conduct annual reviews of their agencies' information security programs, and report the results to the Office of Management and Budget (OMB). As part of this review, OMB requires inspectors general to use 98 security metrics in 11 security areas to assess their agencies' performance.

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices. Specifically, we assessed DOT's (1) information security policy and procedures; (2) enterprise-level information security controls;[1] (3) system-level security controls; and (4) management of information security weaknesses. Also, as required by OMB, we provided our results to OMB via its Web portal.[2]

[1] 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.
[2] OMB designated this information "For Official Use Only." Consequently, our submission to OMB is not contained in this report.

We conducted this audit between February and October 2013 in accordance with generally accepted Government auditing standards. To address OMB's 2013 FISMA reporting metrics, we assessed 60 sample systems, 55 of which we also evaluated during fiscal year 2012. We also performed analytical reviews of data contained in the Department's Cyber Security Assessment and Management system (CSAM),[3] tested software settings in eight general support systems, reviewed supporting documentation, and interviewed Department officials. As part of this audit we selected a statistical sample of 994 out of 79,759 computers that allowed us to project that 83 percent[4] of the DOT computers are compliant with configuration standards.[5] Exhibit A provides more details on our scope and methodology.

RESULTS IN BRIEF

Since our 2012 review, DOT has made progress in its information security program. For example, the Office of the Chief Information Officer (OCIO) issued continuous monitoring guidance, continued to implement the personal identity verification (PIV) program, and began deploying its software for configuration management. However, the Department's information systems remain vulnerable to serious security threats due to the following deficiencies:

1. The Department has not completed its procedural guidance. Specifically, OCIO's enterprise architecture[6] (EA) guidance is not detailed enough to ensure DOT's 13 operating administrations (OA)[7] create effective EA procedures. In addition, OAs have yet to complete information security management procedures, such as continuous monitoring, as required by OCIO's security policy. These gaps in DOT procedures have contributed to the security weaknesses we identified.

2. DOT's enterprise-level controls—controls that must be implemented Departmentwide—are still not adequate to ensure that (1) all contractors receive required security training; (2) personnel with significant security responsibilities receive sufficient specialized training; (3) all possible security incidents are detected and reported to the Department of Homeland Security (DHS), and are remediated promptly; and (4) configuration baselines and

[3] CSAM tracks system inventories, weaknesses, and other security information.
[4] Our estimate has a margin of error of +/-8.4 percentage points at the 90 percent confidence level.
[5] United States Government Configuration Baselines 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.
[6] 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. An EA includes both a baseline (current) and a target (planned) IT structure, and a plan for transitioning from the current to the planned.
[7] See Exhibit C for a list of the OAs, their full names, and their acronyms.

changes are appropriately managed. Furthermore, despite some progress, the Department has not fully complied with configuration standards, including those for Microsoft Windows. DOT also continues to lack a Departmentwide risk management program, and does not sufficiently consider IT security in its investment planning.

3. The Department's system-level controls also remain insufficient to protect system security and ensure systems can be recovered in the event of an emergency shutdown. OAs have not implemented controls for identifying and managing the risks associated with their systems, such as authorization of system operation, coordination of shared security controls, continuous security control monitoring, user identity verification and access control, and contingency planning and testing. Establishing a risk management framework that incorporates such controls is critical to securing DOT's IT systems. The Department also continues to have problems identifying contractor-operated systems and complying with requirements for using cloud computing.

4. Last, the Department still lacks an effective process for timely remediation of security weaknesses. Of the more than 6,700 open plans of action and milestones (POA&M), approximately 37 percent did not have planned start dates, and almost 65 percent—including some that were high priority due to serious risk—did not have remediation costs assigned to them. Furthermore, not all security weaknesses had been reported to CSAM, the central repository that the Department uses to track security weaknesses and their remediation.

We are making a series of recommendations to help the Department establish and maintain an effective information security program—one that complies with FISMA, OMB, and other requirements.

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 another agency, a contractor, or other entity. Similarly, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires Federal agencies to plan for security, 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 454 information systems. DOT 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. The Department must also protect billions of dollars for highway reconstruction, high-speed rail development, and law enforcement grants.

Since 2008, we have reported on weaknesses in DOT's information security program and practices. Over the past 3 years, we reported the following:

- The Department successfully provided security awareness training to over 90 percent of its employees but had not made sufficient progress in other critical areas.[8] In its assurance letter to the President, the Department reported that its non-compliance with FISMA during 2010 constituted a material weakness in internal controls.

- The Department made some improvements in its cybersecurity. It developed a comprehensive cybersecurity policy for the Department, except the Office of the Secretary (OST),[9] and reported all major security incidents to DHS. However, it had not corrected weaknesses in its information security procedures, enterprise-level and system-level controls, and management of corrective actions.[10] Overall, the Department's information security system remained ineffective.

- The Department made improvements to its security controls. Notably, it took steps to enhance the Department's cybersecurity policy and guidance, established a repository for software security baselines, and acquired sophisticated software to improve its security monitoring. However, the Department had not implemented many of the recommendations we made in prior reports that would permit it to meet Federal IT security requirements.[11] As a result, the Department's information systems remained vulnerable to serious security threats and risks.

Exhibit B contains the status of prior year recommendations.

---

[8] *Timely Actions Needed to Improve DOT's Cybersecurity*, OIG Report Number FI-2011-022, November 15, 2010.
[9] In 2011, OST management had differing views on needed policy changes. As a result, the Department excluded OST from DOT-wide security policy. Subsequently, the Department issued OST-specific security policy.
[10] *Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of Its Information Systems,* OIG Report Number FI-2012-007, November 14, 2011.
[11] *Ongoing Weaknesses Impede DOT's Progress Toward Effective Cybersecurity,* OIG Report Number FI-2013-014, November 14, 2012.

OCIO AND OAs HAVE NOT COMPLETED THE REQUIRED SECURITY PROCEDURES

FISMA requires each department's CIO to develop and maintain information security policies and procedures to address security requirements. CIOs may also delegate to their agencies 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 a year. However, OAs have not completed all required procedures. Table 1 highlights important areas that remain outstanding.

Table 1. Significant Deficiencies in Procedures

Security Program Area	OIG Evaluation
Continuous Monitoring of Controls	
Ensures controls remain effective over time.	OAs still need to develop or improve their procedures for performing continuous monitoring.
Risk Management	
Identifies and tests controls, assesses risk, determines whether risks can be accepted, and authorizes the system to operate.	Both OCIO and OAs must develop procedures for accepting and monitoring shared security controls.
Capital Planning and Investment	
Ensures security funding is incorporated into system budgeting.	OAs have not developed procedures for managing security costs as part of their IT capital planning. OCIO also has not developed guidance to assist OAs in creating effective EA procedures.[12]

Source: OIG Analysis

The lack of procedures for implementing security requirements increases the risk that OAs will not properly apply security controls to their information systems. Further, the absence of procedures has contributed to the other security weaknesses we identified.

In its policy, OCIO also delegated authority to OAs to develop supplemental guidance on effective and consistent implementation of information security. However, at the end of fiscal year 2013, not all OAs have completed their OA-specific supplemental guidance. The CIO informed us that his office will review each OA's guidance, once developed, to ensure that it aligns with the Department's policy.

[12] *DOT Does Not Have An Effective Enterprise Architecture Program for Management of Information Technology Changes*, OIG Report Number FI-2012-086, April 17, 2012.

DOT LACKS THE ENTERPRISE-LEVEL CONTROLS NEEDED TO SAFEGUARD ITS IT SYSTEMS

DOT's enterprise-level controls—controls that must be implemented across the Department—remain inadequate. Specifically, DOT lacks the controls needed to ensure all contractors receive required security training, and employees who require specialized training receive it. The Department's efforts to properly detect and report security incidents, appropriately manage configuration baselines, fully address risk, and consider security costs in IT investment planning remain ongoing.

The Department Lacks Data To Track Required Security Training for DOT Contractors

FISMA requires agencies to develop and maintain a comprehensive security training program that ensures all computer users[13] are adequately trained in their security responsibilities before they are allowed access to information systems. However, since 2008, DOT has not adequately tracked the number of contractors it employs and, therefore, does not know how many contractors have completed or need to complete required security training—increasing the risk that contractors will accept malicious codes through social engineering,[14] develop poor passwords, misuse the Internet, or create other security vulnerabilities.

In fiscal year 2013, DOT senior officials again reported that the Department had not implemented a tool to track security awareness training for contractors. The current process for tracking contractor training continues to produce data that differ between OCIO and OAs. Table 2 provides some examples:

Table 2. Examples of Discrepancies in OCIO- and OA-Reported Contractor Data

Discrepancy	OCIO Reported	OA Reported
Number of MARAD contractors	491	123
RITA contractors requiring security training	157	328
FHWA contractors that did not complete security training	211	50

Source: OIG Analysis

[13] Users may include employees, contractors, foreign or domestic guest researchers, other agency personnel, visitors, guests, and other collaborators or associates requiring access.

[14] Social engineering is an attempt to trick someone into revealing information, such as a password, that can be used to attack systems or networks.

Most DOT Personnel With Significant Security Responsibilities Did Not Meet Specialized Security Training Requirements

DOT's cybersecurity policy requires OAs to identify personnel who require specialized security training, such as network administrators and CIOs, and ensure these employees receive a specified number of hours of specialized training. OAs that provided relevant data generally did not meet these requirements (see Table 3).

Table 3. Specialized Security Training

OA	Personnel Who Require Specialized Training	Personnel Who Met Hour Requirements
FHWA	187	5
FRA	43	0
OST	113	2
PHMSA	69	3

Source: OIG Analysis

Six OAs—FAA, FMCSA, FTA, MARAD, NHTSA, and SLSDC—could not provide data on the personnel who received specialized security training or the hours of training that they attended. Furthermore, the Surface Transportation Board (STB) did not and does not plan to provide specialized training for its personnel who require it. OCIO is planning to enforce compliance through a memorandum of understanding with STB. Finally, RITA did not provide evidence that 404 of its employees require specialized training and could not tell us how many actually received training.

This lack of specialized security training makes it difficult for the Department to be sure that personnel with significant security responsibilities develop the skills they need to carry out their responsibilities.

DOT's Incident Reporting and Remediation Practices Reflect Minimal Improvement

DOT's policy requires CSMC to monitor all DOT systems for intrusions, including systems operated by contractors or other Government organizations. CSMC reported that from July 2012 to July 2013, it successfully remediated 1,478 incidents. However, it does not monitor MARAD's U.S. Merchant Marine Academy's network or the Local Area Network at FAA's Aviation Safety subdivision (AVS). Furthermore, during our recent audit of DOT's common

operating environment (COE),[15] we found that CSMC cannot fully monitor the COE because it does not have a complete inventory of network devices. CSMC also cannot scan AVS devices for vulnerabilities because FAA's IT networks and management oversight are not consolidated. FAA officials reported FAA is in the process of consolidating its networks. Finally, the current memorandum of agreement between CSMC and OST outlines network, monitoring and surveillance services, but OCIO does not enforce all of the agreement's requirements. These monitoring gaps impede CSMC's ability to ensure that DOT reports all incidents to the U.S. Computer Emergency Readiness Team (US-CERT),[16] as required by OMB.

OMB requires agencies to respond to incidents in a timely manner to minimize further intrusion. However, DOT has not established remediation timeframes, potentially extending the time systems are exposed to compromise. In some cases, the time it took to complete remediation appears excessive given the risks involved. For example, remediation of denial of service averaged 21 days. See Table 4 for average number of days to remediate incidents, by National Institute of Standards and Technology (NIST) categories.

Table 4. CSMC's Remediation of Security Incidents

NIST Category[a]	Remediated Incidents	Average Days to Remediate after report to CSMC
1 Unauthorized Access	153	19
2 Denial of Service	3	21
3 Malicious Code	933	18
4 Improper Usage	198	14
5 Scans/Probes/Attempted Access	39	25
6 Investigation	150	14

Source: OIG Analysis

[a] Incidents are classified into categories to simplify incident reporting to US-CERT. The categories do not prioritize timeframes for remediation.

DOT Has Not Fully Complied With Configuration Standards

For use of commercial software, OMB requires agencies to comply with U.S. Government Configuration Baseline (USGCB) settings for that software. USGCB has established minimally acceptable, secure system configurations that provide a baseline level of security and ensure the efficient use of resources. While it has made some progress, DOT is still not fully compliant with USGCB settings.

[15] *Security Weaknesses in DOT's Common Operating Environment Expose Its System and Data to Compromise*, OIG Report Number FI-2013-123, Sept. 10, 2013.

[16] US-CERT, managed by DHS, coordinates Federal cyber information sharing and manages cyber risks.

Progress Has Been Made, But Not All Department Computers Comply With USGCB Settings for Microsoft Windows

OMB requires agencies to adopt USGCB settings for Microsoft Windows operating systems, to assess compliance with these requirements, and to be 100 percent compliant. To test DOT compliance, we selected a statistical sample of 994 of 79,759 computers from all OAs, but OAs could not locate 712 of the 994. Based on this, we estimate that OAs could not find 56,376, or 70.7 percent, of the Department's 79,759 computers.[17] This is an increase of 14.3 percentage points from 2012's 56.4 percent.

We tested the remaining 282 computers in our statistical sample for USGCB settings. Based on this, we estimate that 82.9 percent of the approximately 23,383 available computers with Windows software in the Department's universe of computers and servers met baseline settings,[18] up 20 percentage points from 2012's 63 percent. For example, FAA's Air Traffic Organization (ATO) local area network (LAN) passed 80 percent of the controls in the computers we sampled. See Table 5 for details on the controls that passed and failed.

Table 5. 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
COE[b]	68	19,479	17,479	2,000	90%
FAA-ATO LAN	43	9,245	7,396	1,849	80%
FAA-AVS LAN[c]	0	0	0	0	--
FMCSA Service Centers	46	12,125	3,644	8,481	30%
USMMA LAN[d]	2	526	517	9	98%
Volpe Center LAN	43	10,791	10,185	606	94%
STB LAN	26	5,220	1,850	3,370	35%
OIG Infrastructure	54	14,094	13,550	544	96%
Totals	**282**	**71,480**	**54,621**	**16,859**	

Source: OIG analysis

[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 OAs' common network infrastructures (email, desktop computing, and LANs) into a common IT infrastructure.
[c] AVS LAN did not produce any results due to limitations in their scanning capability.
[d] USMMA LAN produced results for only two selected samples due to the high number of unavailable computers.

[17] Our estimate has a margin of error of +/-4.3 percentage points at the 90 percent confidence level.
[18] Our estimate has a margin of error of +/-8.4 percentage points at the 90 percent confidence level.

OMB also requires agencies to submit monthly reports on their maintenance of USGCB baseline security settings. However, DOT's monthly reports to OMB have been incomplete. For example, FAA-AVS has not performed USGCB scanning due to its limited scanning capability—the data is not included in the report to OMB. Furthermore, FAA's security office could not validate the results from ATO's USGCB scanning.

DOT Has Not Implemented All Required Controls for Configuration Management

DOT's cybersecurity policy and NIST policy require OAs to plan, implement, monitor, and report on baseline security standards. We tested 55 systems and found multiple instances in which configuration controls had not been implemented or were only partially implemented, or documentation did not identify whether the control was in place (see Table 6).

Table 6. Sample Systems' Implementation of Configuration Security Controls

NIST Security Control	Configuration			Flaw Remediation	Vulnerability Scanning
	Baseline	Settings	Change Management		
Implemented	40	20	43	33	34
Partially Implemented	6	15	2	9	4
Not Implemented	8	10	5	3	4
Status Unidentified	1	10	5	10	13
Total	**55**	**55**	**55**	**55**	**55**

Source: OIG analysis

DOT Continues To Lack a Comprehensive Departmentwide 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. To date, DOT has only created a Departmentwide governance structure that addresses risk at the system level.

At the system level, some OAs have made progress developing their risk management programs (see Table 7).

Table 7. Risk Management Progress Summary

Risk Management Program Elements	FAA	FHWA	FRA	FTA	OIG	PHMSA
Internal policy documents risk management programs			✓	✓	✓	✓
Defined procedures to execute risk management programs	✓	✓	✓		✓	✓
Established comprehensive governance structures and follow organizationwide risk management strategies	✓	✓			✓	✓
Established criteria for making risked based decisions	✓	✓			✓	✓

Source: OIG analysis

Despite this progress at the system level, the lack of a Departmentwide risk management program that includes governance structures for managing and monitoring risk at all three levels makes it difficult for DOT to understand how information security risk affects its missions and business functions.

The Department's Capital Planning and Investment Control Process Does Not Address IT Security

To ensure an adequate budget for security, the Clinger-Cohen Act of 1996[19] requires agencies to plan for and track information security costs as part of their capital planning processes and to link these costs to their EA. However, DOT has yet to integrate IT security into its capital planning and investment control process—due to OCIO's delay in finalizing the Department's integration policy and procedures, and in providing guidance to OAs on estimating IT security costs. OCIO also informed us that it has not completed the update of its "Integrated Program Planning and Management (IPPM) Governance and Practitioners Guide"—which provides a framework for planning and managing IT programs and projects—to integrate security estimation and management controls. The Department's lack of a security estimation process linked to an EA makes it difficult for the Department to ensure that security funding is cost effective. Table 8 shows DOT's IT security investments by OA.

[19] The Clinger-Cohen Act, formerly the Information Technology Management Reform Act, Pub. L. No. 104-106 (1996) and codified at 40 U.S.C. § 11101, *et seq*. (2011).

Table 8. DOT's IT Security Investments

OA	Number of IT Investments[a]	Total Funding requested for IT investments (in dollars) [a,c]	Total Funding requested for IT security (in millions of dollars) [b,c]	Security cost estimation process established?[d]
FAA	132	$2.7 B	$59.8	No
FHWA	44	57.1 M	2.4	No
FMCSA	18	32.4 M	1.8	No
FRA	21	17.1 M	.6	No
FTA	14	25.6 M	.1	No
MARAD	25	20.2 M	1.5	No
NHTSA	22	40.0 M	.4	No
OIG	2	3.7 M	.3	Yes
OST	55	175.5 M	.6	No
PHMSA	13	20.8 M	.3	Yes
RITA	12	19.9 M	1.3	No
SLSDC	2	230.0 K	.0	Yes
STB	5	1.8 M	.0	No
Total	**365**	**$3.1B**	**$69.0[e]**	

Source: OIG analysis

[a] OMB Federal IT Dashboard FY 2014 Edition Website (www.itdashboard.gov/portfolios), as of September 23, 2013.

[b] DOT's Oracle Primavera Portfolio Management (OPPM) system Website (jamcdfpvap137.amc.faa.gov/prosight/), as of September 24, 2013.

[c] Dollar amounts are rounded.

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

[e] This amount does not include approximately $1.5 million that DOT is requesting for IT investments to support the COE, On Line Rulemaking, and DOT's Cybersecurity Program.

DOT'S SYSTEM-LEVEL CONTROLS ARE INSUFFICIENT TO KEEP SYSTEMS SECURE OR ENSURE RECOVERY

The Department's system-level controls are insufficient 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 for system authorization because OAs have not established risk management frameworks as required by DOT policy.

OAs Have Not Implemented Risk Management Frameworks

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, including authorization of system operation, coordination of shared security controls, continuous monitoring of security controls user identity verification and access control, and contingency planning and testing. OAs have not complied with NIST's risk management framework, as DOT policy requires.

OAs Authorize System Operation without Completing All Security Requirements

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires Federal systems to be reauthorized—or reaccredited—at least once every 3 years. An authorizing officer, typically a senior executive, reviews the certification results and reauthorizes the system when he or she determines that the system's operation poses minimal security risk. However, as of May 2013, 19 DOT systems were unaccredited or not reauthorized to operate—an increase of 8 over fiscal year 2011 (see Table 9).

Table 9. Systems with Expired Authorization to Operate

OA	System	Expiration of Authorization to Operate
FMCSA	SAFER	5/29/2009
	PRISM	5/9/2011
	HMPIP	6/23/2011
	Analysis & Information	4/28/2013
	DataQs	4/28/2013
	FMCSA LAN Segment at Volpe	4/28/2013
	National Consumer Complaints Database	4/28/2013
	SAFETYNET	4/28/2013
	MCMIS	12/5/2008
MARAD	BlackBoard	3/16/2013
	Comprehensive Academic Management System	3/16/2013
	USMMA LAN	3/16/2013
	USMMA Student Information System	3/16/2013
OST	Grants Information System	4/6/2013
	Parking and Transit Benefit System	4/21/2013
RITA	RITA Mission Support	7/30/2009
	RITA Web	5/31/2010
	Transtats	5/16/2011
	TSI Infrastructure	1/2/2010

Source: OIG analysis

OCIO stated that it had approved system owners' requests for extensions for overdue authorizations. However, system owners did not provide all required information with their requests—including information on unresolved POA&Ms, agreements for inherited controls, and annual testing of security controls—and OCIO's compliance review reports did not identify these issues.

Furthermore, 30 of 60 sample systems had incomplete authorization documentation, and 8 had incomplete control testing (see Table 10).

Table 10. Sample Systems' Security Authorization, and Security Control Testing

OA[a]	Systems Tested	Systems Without Adequate Security Authorization	Systems Without Complete Security Control Testing
FAA	22	7	1
FHWA	5	0	0
FMCSA	3	3	3
FRA	2	2	0
FTA	2	2	1
MARAD	3	3	0
NHTSA	2	2	0
OIG	2	0	0
OST	10	5	0
PHMSA	2	0	0
RITA	4	3	3
SLSDC	1	1	0
STB	2	2	0
Total	**60**	**30**	**8**

Source: OIG analysis

[a] For purposes of this report, COE systems are counted under OST.

The lack of proper system security authorization makes it difficult for DOT and OAs to identify and resolve system weaknesses, and consequently, for the Department to ensure that its systems are reasonably protected against security threats.

DOT Has Not Developed Policy and Procedures for the Use of Common Security Controls

All 13 OAs used common controls[20] as part of their systems' security. However, the Department has not made progress in implementing NIST requirements for these controls. Specifically:

- The Department continues to lack procedures for the use of common controls.
- Common control providers have not finalized security plans to guide users when the controls are not effective.
- Common control users do not coordinate with the controls' providers to ensure the controls are effective.
- Common control users frequently do not verify the controls' functionality when they conduct system security authorizations.

Without guidance and security plans, OAs processes for assessing the risks common controls present to their systems may not be comprehensive enough to ensure risks are identified and mitigated. Furthermore, the lack of adequate management of common controls results in systems that are authorized without testing the common controls that they use.

DOT's Continuous Monitoring of Security Controls Remains Insufficient

NIST provides guidance to agencies for implementing a program to continuously monitor security controls. Continuous monitoring provides ongoing awareness of information security, vulnerabilities, and system threats to support risk management decisions. In January 2013, in response to our recommendation, DOT issued the "Security Authorization & Continuous Monitoring Performance Guide." The guide provides Departmentwide monitoring standards and requires OAs to implement continuous monitoring programs that include policy or procedures, security architectures, metrics, monitoring and assessment frequencies, and security status reporting. In 2012, OCIO acquired a complex software solution to assist OAs in continuously monitoring security controls. However, most OAs, including FAA, have not agreed to use the proposed software. Only OST is now using this software—for its common operating environment—but it did not provide evidence that it uses the software's reports to address vulnerabilities.

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

Despite DOT's guidance and new software, none of the OAs has implemented full programs, and only five have implemented one or more of the required program elements (see Table 11). The lack of comprehensive continuous monitoring program diminishes OAs' abilities to identify and respond quickly to system security threats.

Table 11. DOT's Continuous Monitoring Programs

OA	Policy	Architecture	Metrics	Monitoring/ Assessment Frequencies	Status Reporting
FAA	x	x	x	x	x
FHWA	x	x	x	x	x
FMCSA	✓	x	x	x	x
FRA	✓	x	x	x	x
FTA	✓	x	x	x	x
MARAD	x	x	x	x	x
NHTSA	x	x	x	x	x
OIG	✓	x	✓	✓	✓
OST	x	x	x	x	x
PHMSA	✓	x	✓	x	✓
RITA	x	x	x	x	x
SLSDC	x	x	x	x	x
STB	x	x	x	x	x

Source: OIG analysis

DOT Has Made Limited Progress on Implementing Use of Personal Identity Verification Cards for User Access to Systems and Facilities

OMB required that (1) by 2008 all Federal personnel have a PIV card, and (2) by 2012 all Federal personnel use PIV cards to log on to agency computers as part of multifactor user identity authentication. DOT did not meet these deadlines and has not yet completed the Federal PIV initiative. During 2012, DOT increased PIV card issuance to above 97 percent, but provisioning (unique identifiers that associate a card to its holder) remains at only 13 percent. As of June 2013, DOT continued to report shortcomings in the PIV program:

- Only 39 percent of DOT's systems were PIV enabled for user log on, and only 6 percent of its systems require PIV use for user logon. In 2012, we reported higher numbers: 42 percent of DOT's systems were PIV enabled and 7 percent required PIV use for user logon. According to OCIO, the reductions resulted from OAs providing incomplete information during 2013.

- DOT has not adapted all of its facilities to accept PIV cards for facility access. FAA informed us it will upgrade all facilities by the end of fiscal year 2018. OST informed us that it has a rolling plan for other facilities in which each facility will be assessed as funding becomes available.

This lack of full use of PIV cards for user log-in and facility access 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 and Testing Remains Inadequate

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. It must also be updated regularly so that it remains current with system enhancements and organizational changes. In a sample of 60 systems, 11 OAs had deficiencies in their contingency plans for at least one system (see Table 12).

Table 12. Identified Deficiencies[a] in Sample Systems' Contingency Plan Preparation, Training, and Testing, by OA

FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OST	PHMSA	RITA	STB
No Business Continuity and Disaster Recovery Plan (BCDRP) for all systems [b]										
X	X	X	X	X	X	X	X	X	X	X
BCDRP not revised to correct deficiencies found during testing										
	X	X	X	X	X	X	X	X	X	X
Contingency plans not tested										
X	X	X	X	X	X			X	X	X
Contingency test after action report not developed										
X	X	X	X	X	X	X	X	X	X	X
System backup not in accordance with procedures										
	X	X	X	X	X	X	X		X	X
Alternative processing sites vulnerable to the same risks as primary sites										
X	X	X	X	X	X	X	X	X	X	X

Source: OIG analysis

[a] Deficiencies were found in one or more OAs' sample systems.

[b] OAs are required to have a BCDRP for each of their systems.

A lack of rigorous contingency planning and testing inhibits OAs' abilities to recover their systems after unplanned shutdowns and minimize business disruption. Furthermore, this lack of risk management frameworks prevents the

Department and OAs from establishing their information system security with the most recent security best practices recommended by NIST guidance.

Despite Progress, the Department Continues To Have Problems Identifying Contractor-Operated Systems

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. Contractor systems represent higher risk to the Department because it does not manage their security controls.

In fiscal year 2012, OCIO provided OAs with guidance[21] that requires them to correctly identify contractor operated systems. Based on the guidance, OAs recategorized 114 systems. However, we found an additional 108 contractor operated systems that OAs had incorrectly identified as organization operated systems (see Table 13).

[21] "DOT FISMA Inventory Guide," June 2012.

Table 13. DOT's Organization and Contractor System Designation

OA	Total Systems	Designation in CSAM		Contractor Systems Incorrectly Designated
		OA-Operated	Contractor-Operated	
FAA	303	287	16	97
FHWA	21	0	21	0
FMCSA	18	16	2	0
FRA	15	6	9	2
FTA	6	0	6	0
MARAD	22	0	22	0
NHTSA	10	7	3	3
OIG	3	3	0	0
OST[a]	30	3	27	0
PHMSA	7	0	7	0
RITA	17	16	1	6
SLSDC	1	1	0	0
STB	1	1	0	0
Total	**454**	**340**	**114**	**108**

Source: OIG analysis

[a] For purposes of this report, we counted the COE's systems as OST's systems.

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 Have Not Complied With Requirements

Cloud computing enables convenient, on-demand network 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 provided through private offering—exclusive use by the organization—or public offering—the cloud infrastructure is provisioned for open 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.

However, not all OAs using cloud computing provided adequate evidence of their compliance with these requirements. For example, four OAs—MARAD, RITA, FTA and OST—have investments that use cloud computing and have the following issues:

- MARAD and RITA did not provide evidence that they had FedRAMP compliant agreements in place for their investments.

- FTA uses private services managed by OST to host several information systems but has no agreement with OST for the services.

- OST reported that its inventory of investments using cloud computing is inaccurate and that its investments are mislabeled.

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 LACKS AN EFFECTIVE PROCESS FOR THE REMEDIATION OF SECURITY WEAKNESSES

FISMA requires agencies to develop a process to remediate security weaknesses. OMB also 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 risk criteria they developed. DOT policy also requires OAs to record their POA&Ms in CSAM.

In September 2012, DOT issued its Security Weakness Management Guide that provides additional details to OAs on how to report, manage, and monitor security weaknesses. However, DOT's POA&Ms are still not managed in accordance to Federal and Department requirements. OAs have 6,714 open POA&Ms—almost 1,500, or 28 percent, more than last year, some of which date from 2005. For example:

- 2,473 (37 percent) lack planned start dates;

- 4,310 (64 percent), 95 of which were high priority, did not document remediation costs; and

- 1,469 were moderate priority and did not identify costs.

See Table 14 for details.

Table 14. Summary of Open POA&Ms Without Planned Start Dates or Documented Costs (from 2005 through 2013)

OA	Total Open POA&Ms	With No Planned Start Date	With No Documented Costs
COE	43	0	0
FAA	4,624	1,427	2,743
FHWA	115	1	1
FMCSA	1,182	626	1,163
FRA	133	49	94
FTA	25	0	0
MARAD	319	295	159
NHTSA	2	2	0
OIG	3	0	0
OST	96	2	3
PHMSA	3	2	3
RITA	87	44	77
SLSDC	1	0	0
STB	81	25	67
Total	**6,714**	**2,473**	**4,310**

Source: OIG analysis

We identified other noncompliances related to the remediation of security weaknesses:

- Of the 60 sample systems we reviewed, 27 had POA&Ms that OAs had not recorded in CSAM. DOT policy requires OAs to record all known weaknesses in CSAM—a database intended to facilitate tracking of security weaknesses and their remediation.

- A 2010 OCIO-commissioned assessment of COE security did not review COE weaknesses in CSAM.

- OCIO has not complied with FISMA's requirement that department CIOs track open recommendations from their inspectors generals' annual reviews.

- OCIO did not provide evidence that it had complied with OMB's requirement for Federal CIOs to review their agencies' progress on POA&M remediation.

Unresolved POA&Ms make it difficult for DOT to ensure systems are adequately secured and protected, thus creating risk of compromise.

CONCLUSION

While DOT implemented a number of actions to enhance its cybersecurity program, many are incomplete and others have not been initiated. In most cases, overall progress has been slow. Long-standing deficiencies put at risk the confidentiality, integrity, and availability of the Department's information and make it vulnerable to hackers and others who aggressively probe and compromise Federal networks. Until the Department implements corrective actions to remediate weaknesses and comply with Federal requirements, DOT's IT systems will remain exposed to serious security risks.

RECOMMENDATIONS

To help the Department address the challenges in developing a mature and effective information security program, we recommend that the Chief Information Officer take the following actions in addition to 15 recommendations that are still open from prior FISMA reports:

Enterprise-Level Weaknesses

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 OA's processes for configuration management and verify that mitigating activities are initiated, executed, and completed in accordance with DOT policy and NIST guidance. Report exceptions to OA management.

3. 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.

Information System Security

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.

AGENCY COMMENTS AND OIG RESPONSE

We provided a draft of this report to OCIO on November 12, 2013. On November 20, 2013, we received OCIO's response, which can be found in its entirety in the appendix to this report. In its response, OCIO generally concurred with our recommendations and highlighted the progress it made during fiscal year 2013. OCIO also outlined its plan to make its cyber environment as secure as possible and its commitment to providing us with specific planned actions and milestones to address our recommendations. The Office will provide to us, by January 31, 2014, specific responses to each recommendation that identify and prioritize planned actions and anticipated milestones.

ACTIONS REQUIRED

We believe that OICO is responding to our recommendations. However, we must review OCIO's January 31, 2014 submission to determine whether the Office's specific planned actions and anticipated milestones satisfy the intent of each recommendation. Based upon this review, we will also determine whether the recommendations are resolved but open pending completion of the planned actions and milestones. All corrections are subject to follow-up provisions in DOT Order 8000.1.C.

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; Lou E. Dixon, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-1427; or Louis C. King, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

cc: Deputy Secretary
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 60 of 454 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 15 for sampled systems and Table 20 for all systems). We planned to test the same 60 systems we tested in the prior year. Of those systems, 55 were available but 5 were retired. To replace the retired systems, we used 5 of the prior year sample's substitute systems. To evaluate USGCB compliance, we selected a statistical sample of 994 of 79,759 devices to scan for compliance. We created a script to extract the test results of USGCB controls from 282 of 994 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, 2013. We performed our information security review work between February 2013 and November 2013. 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 15. OIG's Representative Subset of DOT Systems, by OA

No.	System	Impact Level[a]	Contractor System?[b]
Federal Aviation Administration			
1	Whistleblower Protection Program	High	X
2	Inspector Credentials	High	X
3	Web Operations Safety System	High	X
4	Safety Risk Management Tracking System	Low	X
5	Bandwidth Manager	Moderate	X
6	AST Local Area Network	Moderate	X
7	Air Route Surveillance Radar Model 4	Moderate	X
8	ASH External Web Portal	Moderate	X
9	Safety Management Information System	Moderate	X
10	Interim Voice Switch Replacement System	Moderate	X
11	Advanced Qualification Program	Low	X
12	Obstruction Evaluation/Airport Airspace Analysis	Low	X
13	Safety Issues Reporting System	Moderate	X
14	Monitor Safety Analyze Data	Moderate	X
15	FAA Read-Only Data Interface	Moderate	✓
16	Real Estate Management System	Moderate	X
17	Enterprise Architecture & Solutions Environment	Moderate	✓
18	ATO Application Portal	Moderate	X
19	Messaging Services	Moderate	X
20	Data Multiplexing Network	Moderate	X
21	Technical Support Services Contract- Work Release Information Tracking System	Low	X
22	Enhanced Terminal Voice Switch	Moderate	X

No.	System	Impact Level[a]	Contractor System?[b]
Federal Highway Administration			
23	Rapid Approval & State Payment System	High	✓
24	ITD Application and Oracle Database Servers	High	✓
25	FHWA Organization Information System	Moderate	✓
26	Motor Fuels and Finance Analysis System – Highways	Low	✓
27	Federal Lands Labor Cost Distribution Process	Low	✓
Federal Motor Carrier Safety Administration			
28	Safety and Fitness Electronic Records	Moderate	✓
29	Hazardous Material Package Inspection Program	Moderate	✓
30	Performance and Registration Information Systems Management	Moderate	✓
Federal Railroad Administration			
31	Automated Track Inspection System	Moderate	✓
32	Locomotive Engineer Training Simulator	Low	✓
Federal Transit Administration			
33	TEAM	Moderate	✓
34	FTA Inter/Intranet	Moderate	✓
Maritime Administration			
35	Maritime Service Compliance System	Moderate	X
36	Electronic Invoice System	Moderate	X
37	FOIAXpress	Low	✓
National Highway Traffic Safety Administration			
38	EDS	Moderate	X
39	Artemis	Moderate	X
Office of Inspector General			
40	US DOT/OIG Infrastructure	Moderate	X
41	US DOT/OIG TIGR System[c]	Moderate	X
Office of the Secretary of Transportation			
42	Drug and Alcohol Testing Management Information System	Moderate	✓
43	Facilities and Building Management System	Moderate	✓
44	Web Printing System	Moderate	✓
45	CASTLE	Moderate	✓
46	Cyber Security Assessment and Management	High	✓
47	Security Operations Systems	High	✓
Pipelines and Hazardous Materials Safety Administration			
48	Hazardous Materials Information System	Moderate	✓
49	PHMSA Portal System	Moderate	✓
Research and Innovative Technology Administration			
50	RITA Mission Support	Moderate	X

No.	System	Impact Level[a]	Contractor System?[b]
51	IEC Data Warehouse	Moderate	X
52	Transtats	High	X
53	Airline Reporting Data Information System	High	X
Saint Lawrence Seaway Development Corporation			
54	Financial Management System	Low	X
Surface Transportation Board[d]			
55	Case Management System	Moderate	X
56	Local Area Network	Moderate	X
Common Operating Environment			
57	Common Operating Environment[e]	High	✓
58	Business Communications System[f]	Moderate	X

Source: OIG

[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 definition of contractor system

[c] Subsequent to our review, OIG's TIGR was shut down.

[d] For purposes of this report, STB was selected as part of the sample. Exhibit C defines STB's obligation to comply with DOT requirements.

[e] The COE is made up of three components, the campus area network, computing services, and helpdesk services.

[f] BCS has been merged into the COE.

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

- *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.

Exhibit A: Scope and Methodology

- *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

EXHIBIT B. Status of Prior Years' Recommendations

Table 16. 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 17. Status of OIG's Recommendations for Fiscal Year 2011

No.	Status	Recommendation
1	Partially Closed	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.
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 18. 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 Department-wide 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.

Exhibit B. Status of Prior Year's Recommendations

No.	Status	Recommendation
5	Closed	Require OST to implement required system patches on their Delphi system.
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 Cyber Security 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.

Exhibit B. Status of Prior Year's Recommendations

No.	Status	Recommendation
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.
22	Closed	In conjunction with the Assistant Secretary for Administration, develop a Department-wide 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	Open	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 19. 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.

No.	Status	Recommendation
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.
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 Cyber Security Assessment and Management system.
18	Closed	Ensure that Maritime Administration properly inventories its information systems and tracks them in the Cyber Security 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.

Exhibit B. Status of Prior Year's Recommendations

No.	Status	Recommendation
27	Closed	Implement NIST-approved encryption on all mobile computers/devices.

Source: OIG
[a] Replaced with 2011 Recommendation No. 3
[b] Merged into 2010 Recommendation No. 23

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

Table 20. System Inventory Counts for Fiscal Years 2012 and 2013

Organization[a]	Fiscal Year	
	2012	2013
Common Operating Environment (COE)	3	1
Federal Aviation Administration (FAA)	284	303
Federal Highway Administration (FHWA)	21	21
Federal Motor Carrier Safety Administration (FMCSA)	18	18
Federal Railroad Administration (FRA)	15	15
Federal Transit Administration (FTA)	5	6
Maritime Administration (MARAD)	22	22
National Highway Traffic Safety Administration NHTSA)	10	10
Office of Inspector General (OIG)	3	3
Office of the Secretary (OST)	28	29
Pipeline and Hazardous Materials Safety Administration (PHMSA)	7	7
Research and Innovative Technology Administration (RITA)	15	17
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)[b]	2	1
Total Systems	**434**	**454**

Source: OIG, and DOT CSAM as of September 27, 2013

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

[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 the Department of Transportation. Accordingly, STB is not obligated to utilize IT security policies or procedures provided by the Department of Transportation.

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
Felicia Moore	Information Technology Specialist
Jenelle Morris	Information Technology Specialist
Jason Mott	Information Technology Specialist
Nileshkumar Patel	Information Technology Specialist
Gary Fishbein	Referencer
Petra Swartzlander	Senior Statistician
Megha P. Joshipura	Statistician
Karen Sloan	Communication 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 Office of Inspector General (OIG) Draft Report on Federal Information Security Management Act 2013

DATE: NOVEMBER 19, 2013

FROM: Richard McKinney
DOT Chief Information Officer

REPLY TO Attn. of:

TO: Calvin l. Scovel III
Inspector General

DOT's Commitment to Cybersecurity as a Priority

As the new Chief Information Officer (CIO) of the Department of Transportation (DOT), I am committed to making cybersecurity the top priority. To demonstrate our commitment to improve our security posture during 2013, we've already made improvements through the issuance of new guidance on continuous monitoring, security authorization, and risk management. The Department has also made progress on Administration Cybersecurity Cross Agency Priority goals to include: Increasing continuous monitoring capabilities across 57% of agency assets; improving implementation of Trusted Internet Connection capabilities from 62% to 72%, and; increasing required use of PIV cards to securely access DOT networks from 0% to 7% in the span of a single quarter. My Office has also submitted evidence for and requested closure to the majority of open FISMA audit recommendations from previous years.

This renewed emphasis on improving the security of our environment acknowledges the significance of the OIGs findings around cybersecurity this year, which we have already begun to address. For example, DOT has made significant strides in making its Common Operating Environment safer, with the addition of tighter controls, greater emphasis on continuous monitoring, and investing resources in better hardware and software. These recent advancements balance the increasing risk threshold to DOT against the resources at our disposal. We continue to improve the Department's cybersecurity posture while

simultaneously maintaining critical operational systems and responding to a significant number of new information technology requirements set by the Office of Management and Budget (OMB).

While generally concurring with the recommendations provided by the OIG in this year's report, we would like to comment on a few areas where OIG provided findings:

- The report identifies weaknesses in the Enterprise Architecture (EA) guidance of the Department — that it was not detailed enough to ensure DOT's 13 operating administrations (OA) create effective EA procedures. In a previous OIG EA report[1], my office expressed its commitment to improving EA, and we are making progress on the recommendations as described in our response. Further, on November 5, 2013, the OMB Federal Chief Enterprise Architect provided comments on the DOT IRM Plan, EA Roadmap, and EA Program granting DOT an overall score of 3.4/4.0. OMB stated that the EA Roadmap and IRM Plan were in the top third of all cabinet level federal government agencies. We will continue to focus on the integration of security into the Enterprise Architecture, as has been reflected in the plans, roadmap and overall program.

- We recognize the need to ensure that appropriate Federal and Contract personnel receive appropriate security training, a risk-based decision consistent with NIST standards. DOT is committed to continuing discussions with the OIG on discrepancies between the way we believe we successfully identify and track role-based security training, and the way the OIG interprets its completion.

- We ensure that the Department reports its incidents within required timeframes to US-CERT. In addition to the current capabilities we already have at our Trusted Internet Connections, we will continue to work to further improve visibility and remediation times within our component operating administrations (OAs). We have also established a Departmental configuration management program based on Federal policy, which requires use of USGCB and has an established process and workflow for documenting and approving deviations.

- We are also leveraging the Department of Homeland Security Continuous Diagnostics and Mitigation services this year, as part of its overall Information Security Continuous Monitoring Program. This will extend the guidance on

[1] DOT Does Not Have An Effective Enterprise Architecture Program For Management of Information Technology Changes, Report Number: FI-2012-086, Issued: April 17, 2012

implementing the Risk Management Framework DOT provided to OAs to provide additional tools, training and integration services that will improve our holistic security posture. In addition to this, we are also working to ensure that cloud services, either currently implemented or in the acquisition process, will meet FedRAMP requirements by the June 5, 2014 deadline.

Improving our cybersecurity posture will require gaining commitment throughout the Department to make our cyber environment as safe and secure as possible. Getting the basics right is key to successfully achieving this goal so we are using a comprehensive team approach to planning and implementing the foundational elements along with developing longer term plans. Making sure that we understand the relevance of the findings and their relationship to the recommendations is critical to developing actionable mitigation strategies to improve our posture.

We intend to provide, under separate cover, by January 31, 2014, a specific response to each recommendation that identifies and prioritizes actions planned and anticipated milestones. Prioritization will factor in consideration of the OIG's work, Government-wide priorities, 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 priorities and continue to meaningfully improve its cybersecurity posture. Please contact Joe Albaugh (joe.albaugh@dot.gov, 202.366.9201) in the Office of the Chief Information Officer with any questions.