Office of Inspector General

Audit Report

FISMA 2012: ONGOING WEAKNESSES IMPEDE DOT'S PROGRESS TOWARD EFFECTIVE INFORMATION SECURITY

Department of Transportation

Report Number: FI-2013-014
Date Issued: November 14, 2012

Memorandum

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

Subject: ACTION: FISMA 2012: Ongoing Weaknesses Impede DOT's Progress toward Effective Information Security
Report Number: FI-2013-014

Date: November 14, 2012

From: Calvin L. Scovel III
Inspector General

Reply to Attn. of: JA-20

To: Acting Chief Information Officer

The Department of Transportation's (DOT) operations rely on more than 400 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. Recently, the Government confirmed that foreign cyber hackers have successfully gained access to some critical Federal infrastructure systems.

To protect the IT systems that support Federal operations, 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 agency's 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 96 security metrics in 11 security areas to assess their agency's performance.

Consistent with FISMA and OMB requirements, our overall 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

[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.

controls; and (4) management of information security weaknesses. Also, as required by OMB, we provided our results via its Web portal.[2]

To conduct our audit and address OMB's 96 metrics, we tested a statistical sample of 58 of 420 systems, performed analytical reviews of data contained in the Department's Cyber Security Assessment and Management system (CSAM),[3] tested software settings in 56 general support systems, reviewed supporting documentation, and interviewed departmental officials. We conducted this audit between February and October 2012 in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology.

RESULTS IN BRIEF

Since our 2011 review, DOT has made improvements to its security controls. Notably, it took steps to enhance the Department's cyber security policy and guidance, established a repository for software security baselines, and acquired sophisticated software to improve its monitoring of security. However, the Department has not implemented many of the recommendations we made over the past several years that would permit it to meet Federal IT security requirements, specifically 21 of 35 open recommendations made since 2009 remain open (see Exhibit B). As a result, the Department's information systems remain vulnerable to serious security threats and risks due to the following continued deficiencies in DOT's information security policies, procedures, controls, and remediation measures:

1. The Office of the Chief Information Officer (OCIO) has completed its high-level security policy and direction to operating administrations (OA) to develop their internal procedural guidance to manage information security effectively. However, the OAs' CIOs are still in the process of completing information security procedures for several key areas, including capital planning for IT security. These gaps in DOT procedures have contributed to the other weaknesses we identified.

2. DOT's enterprise-level controls—those that must be implemented Departmentwide—are still inadequate to ensure (1) that all contractors receive required security training, (2) sufficient coverage of DOT networks for detecting and reporting security incidents to the Department of Homeland Security (DHS), (3) reported incidents are remediated promptly, and (4) configuration baselines and configuration changes are appropriately managed. The Department took a key step in creating a repository of approved secure

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

[3] CSAM tracks the system inventory, weaknesses, and other FISMA security information.

software settings. Still, based on our testing of the 340 randomly selected computers, we estimate that 63 percent[4] satisfy the requirements for control setting compliance, a decline of approximately 7 percentage points from 2011. In addition, enterprise-level cyber security risks have not been addressed, and security costs were not considered when planning IT investments. For example, DOT requested $113 million for IT security as part of its budget process; however, these requests were not supported by a capital planning process or linked to an enterprise architecture (EA).[5]

3. The Department's system-level controls are also insufficient to protect its systems' security and ensure that systems can be recovered in the event of a serious breach. Deficiencies remain in certification and accreditation (C&A), contingency plan testing, and monitoring of security controls for changes. For example, we project that 118 of 420 systems[6] had incomplete C&A documentation. We also project that OAs did not complete contingency testing for 202 systems.[7] Furthermore, the Department does not coordinate shared system security controls, and lacks adequate controls over continuous monitoring, oversight of contractor-operated systems, remote access, and account management. For example, the Department continues to be deficient in implementing the use of two-factor authentication to secure remote access to its systems. To better monitor weaknesses and enhance system security, the Department has acquired a highly complex software tool which, if implemented properly, will enable management to more quickly identify and remediate security threats.

4. The Department still lacks an effective process for timely remediation of security weaknesses. Of the 5,265 open plans of action and milestones (POA&M), 2,161 had passed their due dates for resolution; 432 are a year overdue.

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.

[4] Our estimate has a margin of error of +/-26 percentage points at the 90 percent level of confidence.
[5] An EA defines the 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. EA includes a baseline (as-is) and target (to-be) architecture, and a sequencing plan.
[6] Our estimate has a margin of error of +/-38 systems or 9.0 percentage points at the 90 percent level of confidence.
[7] Our estimate has a margin of error of +/-51 or 12.2 percent at the 90 percent level of confidence.

BACKGROUND

FISMA requires each Federal agency's information security program to secure the information and information systems that support the agency's operations, including those provided or managed by another agency, a contractor, or other entity. FISMA also requires each agency to report annually to OMB, Congress, and the Government Accountability Office (GAO) on the effectiveness of its information security policies, procedures, and practices. In its Circular A-130, Appendix III, "Security of Federal Automated Information Resources," OMB requires Federal agencies to plan for security, ensure that appropriate officials are assigned security responsibilities, periodically review the security controls in their information systems, and authorize system processing prior to operations and periodically thereafter.

DOT's 13 OAs collectively manage 428 information systems, about two-thirds of which are managed by FAA (see Exhibit C). DOT relies on these systems to carry out its complex mission, including ensuring safe air traffic control operations, preventing unqualified drivers from obtaining commercial driver's licenses, and identifying safety defects in vehicles, as well as protecting billions of dollars in funds for highway reconstruction, high-speed rail development, and law enforcement grants.

Since 2002, we have reported on weaknesses in DOT's information security program and practices. In our three most recent reports, we reported the following:

- **November 2009**: We reported that DOT had issued its information security policy—the first step in the development of a sustainable information security program—and improved its Common Operating Environment's[8] (COE) compliance with the Federal Desk Core Configuration (FDCC).[9] However, the Department had not made sufficient progress in other areas. Its security program did not meet all Federal requirements and was not as effective as it should have been.[10]

- **November 2010**: We reported that the Department had successfully provided security awareness training to over 90 percent of its employees, but had not made sufficient progress in other critical areas.[11] In its assurance letter to the

[8] COE is a network that provides DOT headquarters and most OAs with common IT services, such as e-mail.

[9] FDCCs 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. OMB has mandated agencies to adopt these settings. Subsequently, the FDCCs were expanded and called the United States Government Configuration Baseline (USGCB).

[10] OIG, *Audit of DOT's Information Security Program and Practices*, FI-2010-023, November 18, 2009.

[11] OIG, *Timely Actions Needed to Improve DOT's Cybersecurity*, FI-2011-022, November 15, 2010.

President, the Department reported that its non-compliance with FISMA during 2010 constituted a material weakness in internal controls.

- **November 2011:** We reported that the Department had made some improvements in its cyber security. It had developed comprehensive cyber security policy for the entire Department, except for the Office of the Secretary (OST), 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.[12] Overall, the Department's information security system was still not effective.

The most significant change to this year's metrics is that DHS categorized each metric as a President's Administration priority, a key FISMA metric, or a baseline question[13] to assist agencies in prioritizing actions to address information security weaknesses.

DESPITE IMPROVEMENTS, DOT'S INFORMATION SECURITY POLICIES AND PROCEDURES REMAIN INCOMPLETE

FISMA requires each department's CIO to develop and maintain information security policies, procedures, and control techniques to address security requirements. In prior reports, we recommended revisions to DOT's policies that direct its OAs' security efforts. During 2012 and in response to our recommendations, OCIO:

- issued a cyber security policy for OST;
- issued the Interim Security Weakness Management Guide;
- issued the FISMA Inventory Guide which defines information systems and provides guidance on how to identify them; and
- developed a SharePoint site to collect OA cyber security procedures.

Also, in response to our prior three reports, OCIO delegated authority to the OAs to develop supplemental guidance for how to effectively and consistently implement information security. However, as of the end of fiscal year 2012, the guidance remains incomplete. The CIO informed us that his office will review each OA's guidance, once developed, to ensure it aligns with Departmental policy. Table 1 highlights the most important areas that remain outstanding.

---

[12] OIG, *Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of Its Information Systems*, FI-2012-007, November 14, 2011.

[13] Administration Priorities are metrics for Trusted Internet Connection capabilities and utilization, mandatory authentication and Personal Identify Verification (PIV), and continuous monitoring. The next tier is Key FISMA Metrics which include areas such as cloud, remote access, and incident detection. The final tier is Baseline metrics, which are used to establish current performance to be used to evaluate future performance.

Table 1: Most Significant Deficiencies in Procedures

FISMA Security Program Area	OIG Evaluation
Certification and Accreditation (C&A) of Controls	
The assessment of security controls to determine if the controls have been implemented effectively.	Procedures for accepting and monitoring shared security controls have not been developed.
Continuous Monitoring of Controls	
Part of the security authorization process to ensure that controls remain effective over time.	Procedures are in draft and require additional detail to guide OA personnel in the development of monitoring practices.
Capital Planning and Investment	
Policy and procedures that ensure that security funding is incorporated into system budgeting.	Procedures for management of security costs as part of IT capital planning are not developed. In addition, there are not procedures to develop an EA.

Source: OIG Analysis

The lack of adequate procedures on security requirements creates the possibility that security controls will not be properly applied throughout the Department to protect information systems. Absence of procedures has contributed to the other weaknesses we identified.

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

DOT's enterprise-level controls are still inadequate to ensure that contractors receive required security training, security incidents are detected and reported, configuration baselines are appropriately managed, risks are addressed at all levels of the Department, and that security costs are considered when planning IT investments.

DOT Cannot Accurately Track Contractors' IT Security Training

FISMA requires agencies to develop and maintain a comprehensive security training program that ensures that all computer users[14] are adequately trained in their security responsibilities before they are allowed access to agency information systems. In prior years, we have reported that DOT's controls for tracking the number of contractors it has employed are inadequate, resulting in the inability to track training completion for contractors. Over the past year, OCIO has taken a significant step in this area by entering a memorandum of understanding with FAA that requires FAA to maintain a Web site, Sat.DOT.Gov, where all DOT contractors can take the required security awareness training. FAA also maintains

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

a repository of statistics on about 13,000 DOT contractors who have received security awareness training.

However, DOT cannot ensure that all contractors are taking required training due to several weaknesses. First, OAs do not reconcile the number of contractors on board to those who FAA reports as having received training. Second, DOT lacks a robust process to ensure all contractors are identified. Third, some contractors cannot access Sat.DOT.Gov for various reasons, including a lack of user identifications and passwords for log in. Finally, DOT does not address security training for contractors who do not have access to systems because of services they provide, such as security guards. The lack of proper computer security training for contractors creates a risk for several vulnerabilities, including ID and password sharing, acceptance of malicious code through phishing or social engineering, poor password development, and Internet misuse.

DOT's Incident Reporting and Remediation Process Remain Insufficient

DOT policy requires the Department's Cyber Security Management Center (CSMC) to have full network visibility over all DOT systems, including systems operated on behalf of the OAs by contractors and other government organizations. CSMC reported that from October 1, 2011, to September 14, 2012, it successfully remediated 1,969 incidents. However, it does not monitor all departmental networks—including the United States Merchant Marine Academy's (USMMA) network and many of FAA's networks—for intrusions. These monitoring gaps impede CSMC's ability to ensure all incidents are reported to US-CERT[15] as required by OMB and to remediate all possible security incidents.

OMB requires agencies to respond to incidents in a timely manner to minimize further damage. However, DOT policy does not address remediation timeframes. In some cases, the time it took to complete remediation appears excessive given the risks involved. For example, remediation of unauthorized access (Category 1)[16] averaged 20 days; while incidents of malicious code (Category 3) averaged 17 days (see Table 2).

[15] The United States Emergency Readiness Team—or US-CERT—is a system managed by the Department of Homeland Security to coordinate cyber information sharing and proactively manage cyber risks to the Nation while protecting its citizens' constitutional rights.

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

Table 2: CSMC's Remediation of Security Incidents during Fiscal Year 2012, by Category

US-CERT Category[a]	Remediated Incidents	Average Days to Remediate
0 Exercise/Network Defense Testing	6	2
1 Unauthorized Access	151	20
3 Malicious Code	1,320	17
4 Improper Usage	274	10
5 Scans/Probes/Attempted Access	72	14
6 Investigation	146	21

Source: OIG Analysis

[a] No incidents in Category 2 (Denial of Services) were reported.

The lack of comprehensive network monitoring makes it difficult for DOT to ensure that all security incidents are detected, reported, and resolved. Furthermore, the lack of timeframes for resolution increases the risk that critical incidents will not be resolved in a timely manner and expose systems to unnecessary compromise for an excessive amount of time.

DOT Has Not Made Progress in Meeting Configuration Standards

OMB requires compliance with minimally acceptable system configuration requirements for commercial software. Configurations that meet these requirements provide a baseline level of security and ensure the efficient use of resources. To improve the Department's compliance, OCIO created a repository of approved software configurations and a process to review departures from the required settings. However, we found deficiencies in DOT's compliance with the U.S. Government Configuration Baseline (USGCB) settings, and incomplete implementation of other configuration standards throughout the Department. Inadequately configured software also increases security vulnerabilities that could impact DOT's mission and business operations.

OAs' Commercial Operating Systems Do Not Comply With USGCB Security Requirements

OMB requires agencies to adopt USGCB for Microsoft Windows operating systems and to assess compliance with these requirements. OMB further requires agencies to be 100 percent compliant. However, not all DOT systems are configured to meet these requirements. We selected a statistical sample of 1,257 of 82,963[17] computers from all OAs except the Surface Transportation Board

[17] We obtained the universe of computer devices from a proprietary database known as Active Directory.

(STB).[18] OAs could not locate 917 of the 1,257 computers. Based on this, we estimate that OAs could not find or test 56.4 percent, or 46,791[19] of 82,963 total computers during compliance scanning. As a result, OAs cannot determine if these computers comply with USGCB settings. We tested the remaining 340 sampled Windows computers for these settings. Based on this, we estimate that 63 percent[20] of the approximately 36,150 available Windows computers in the Department's universe of computers and servers[21] met baseline settings. This is a decline of 7 percentage points from 2011. See Table 3 for details on the controls that passed and failed.

Table 3: Results of Sample Testing on USGCB for Windows Operating Systems

Component General Support Systems[a]	Computers Sampled	Tested	Passed	Failed	Percent Passed
FAA	127	27,981	14,781	13,200	53%
Federal Motor Carrier Safety Administration (FMCSA) Field Sites	54	8,928	5,331	3,597	60%
COE[b]	60	14,454	5,079	9,375	35%
John A. Volpe National Transportation Systems Center	36	6,304	3,326	2,978	53%
USMMA	17	4,437	4,346	91	98%
OIG	46	11,960	11,465	495	96%
Totals	**340**	**74,064**	**44,328**	**29,736**	

Source: OIG Analysis

[a] OMB Circular A-130, Appendix III, defines 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 local area networks) into a common IT infrastructure.

One of the Department's controls for ensuring the use of these approved configuration settings is the application of uniform approved USGCB settings to all workstations. However, we found that these settings varied between workstations. For example, we found up to 45 different settings on workstations within FAA, the Maritime Administration (MARAD), the National Highway Traffic Safety Administration (NHTSA), and the Federal Highway Administration (FHWA).

In addition, DOT's reports on its maintenance of USGCB baseline security settings, which OMB requires departments to submit monthly, have been

[18] The STB CIO did not provide information due to IT resource constraints. Exhibit C defines STB obligation to comply with DOT requirements.

[19] Our estimate has a margin of error of +/-5.2 percentage points at the 90 percent level of confidence.

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

[21] We tested to verify USGCB settings for the Windows Operating System.

incomplete. For example, COE and CSMC reports showed that tests for USGCB settings were not run or were incomplete for two-thirds of the COE and CSMC workstations in our sample. This occurred in part because some workstations under COE's responsibility were not configured to allow automated testing.

OAs' Configuration Management Procedures Do Not Comply With OMB Policy

OMB requires agencies to develop configuration management policies that include approval and documentation of configuration changes to both hardware and software. In addition, OMB recommends the use of automated tools to manage and communicate configuration changes. However, STB did not provide adequate evidence of approvals for system changes. Furthermore, the Federal Motor Carrier Safety Administration's (FMCSA) field sites do not use computer applications to track and record network changes; this is performed manually.

NHTSA and the Saint Lawrence Seaway Development Corporation (SLSDC) rely on COE for all of their configuration management controls. However, the Department has not implemented a number of these key controls. For example, the COE's configuration baselines are not up-to-date, and its configuration changes are not documented or approved by the COE manager.

DOT Has Not Implemented a Departmentwide Risk Management Program

OMB requires agencies to implement a risk management program that includes a governance structure for managing and monitoring risk at three levels: enterprise, business process, and system. However, DOT has not created this enterprisewide governance structure, and only addresses risk at the system level as part of the certification and accreditation process.

Similarly, OAs, with the exception of NHTSA and the Pipeline and Hazardous Materials Safety Administration (PHMSA), do not have risk management programs and only address risk when accrediting systems. This limited view will likely result in an inadequate understanding and consideration of how information security risk, like other organizational risks, affects the likelihood of DOT successfully carrying out its missions and business functions.

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

During fiscal year 2012, DOT requested $113 million for IT security from OMB—an approximate increase of $15 million over its fiscal year 2011 request.

To ensure an adequate budget for security, OMB requires agencies to plan for and track information security costs as part of their capital planning process and to link these costs to the agencies' enterprise architectures. However, DOT's requests were not supported by a capital planning process or linked to an EA. Furthermore, only NHTSA and SLSDC have a process to estimate security costs (see Table 4).

Table 4: OAs' IT Security Funding Estimation Process

OA	Total IT investment, dollars in millions	Security investment, dollars in millions	Security Cost Estimation Process[a]
FAA	$2,764.07	$72.92	Partial
FHWA	46.99	6.43	Partial
FMCSA	24.20	1.28	Partial
FRA	18.83	1.59	Partial
FTA	18.56	.46	No
MARAD	13.35	1.11	No
NHTSA	24.74	.96	Yes
OIG	3.95	.09	No
OST	154.22	26.92	No
PHMSA	9.09	.43	Partial
RITA[b]	16.62	.95	No
SLSDC	.16	.04	Yes
STB	2.13	0	No
Total	**$3097**	**$113**	

Source: WorkLenz–the Department's investment portfolio system, as of September 2012.

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

[b] Research and Innovative Technology Administration

DOT has not provided OAs with guidance on estimating IT security costs or implemented controls to ensure these costs are reasonable. OAs self-report their security estimates to OCIO for reporting to OMB and are not accountable for the reasonableness of their estimates. OCIO reported that as part of its changes to the Department's EA, which it plans to complete by the end of fiscal year 2014, it is integrating IT security into capital planning and investment control. However, OCIO provided no plan for these efforts or policy and procedures for the integration of EA and IT security into the capital planning and investment control process. In addition, OAs reported that they have not received direction from the OCIO on the development of the EA. Without a security estimation process linked to capital planning and EA, the Department is unable to ensure that funding for critical security needs is cost effective.

DOT'S SYSTEM-LEVEL CONTROLS ARE NOT SUFFICIENT 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 continue to impede DOT efforts to comply with requirements for C&A and contingency plan testing, shared system security controls, continuous monitoring of security controls, oversight of contractor-operated systems, and controls over remote access and identity and account management.

Certification and Accreditation Process and Contingency Plan Testing Are Incomplete

As of September 2012, 11 DOT systems were unaccredited, meaning they were not authorized to operate (see Table 5). 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 through a C&A process. Certification of a system requires assessing risk, planning security, testing of minimum security controls, creating plans of actions for identified weaknesses, and mitigating risks. An authorizing officer appointed by the agency, typically a senior executive, reviews the certification results and reaccredits the system when he or she determines that the system's operation poses minimal security risk. DOT's 11 unaccredited systems represent an increase over last year's 8 unaccredited systems. Of the 11, 4 have been overdue since 2010 and one since 2009.

Table 5: DOT Systems with Expired C&A

OA	System	Expiration Date	Total Systems
FMCSA	Analysis and Information	6/26/3012	
	Safety and Fitness Electronic Records	5/29/2012	
	SAFETYNET	3/16/2012	3
FRA	Procurement Information System for Management	9/10/2012	1
NHTSA	FARS	5/14/2012	1
OST	Correspondence Control Management System	10/31/2010	1
RITA	Mission Support	7/30/2009	
	Transportation Safety Institute Infrastructure	1/02/2010	
	Web	5/31/2010	
	Transtat	5/16/2011	4
STB	Case Management System	11/6/2010	1
Total			**11**

Source: OIG Analysis

We evaluated a random sample of 60 of DOT's 420 IT systems.[22] We found that 24 of the 60 sample systems had incomplete C&A documentation, and 31 systems did not receive complete security control testing. Based on these results, we estimate that 118 of 420 systems[23] in the DOT universe had incomplete C&A documentation and 169[24] did not receive complete security control testing (see Table 6).

Table 6: Sample Systems' C&A, Control Testing, and Contingency Plans

OA	Systems tested	Systems without adequate C&A	Systems without complete control testing	Systems with deficient or inadequate contingency plan/testing
FAA	22	3	5	8
FHWA	5	2	5	2
FMCSA	3	3	3	3
FRA	2	2	0	1
FTA	2	1	2	0
MARAD	3	3	3	3
NHTSA	2	0	0	0
OIG	2	2	2	1
OST[a]	10	4	4	5
PHMSA	2	0	0	2
RITA	4	3	4	4
SLSDC	1	0	1	0
STB	2	1	2	2
Total	**60**	**24**	**31**	**31**

Source: OIG Analysis

[a] For purposes of this report, COE systems are counted under Office of the Secretary.

DOT also lacks a plan for the recovery of its IT systems in the event of a disruption. Both NIST and OMB require Federal agencies to implement plans for recovering their information systems after unforeseen shutdowns. Agencies must also annually test their contingency plans to ensure the plans will function properly when needed. Thirty-one of the 60 systems in our sample had missing or inadequate contingency plans or plan testing. Table 7 provides some examples.

[22] We selected a random sample of 58, or 4.5 percent, of DOT's systems. One system was made up of three subsystems, 1) Campus Area Network, 2) Common Operating Environment, and 3) Helpdesk, bringing our sample to 60 systems.

[23] Our estimate has a margin of error of +/-38 system or 9.0 percent at the 90 percent level of confidence.

[24] Our estimate has a margin of error of +/-44 system or 10.4 percent at the 90 percent level of confidence.

Table 7: Sample Systems' Contingency Plans Preparation, Training, and Testing Results with Identified Deficiencies by OA

Description[a]	FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OIG	OST	PHMSA	RITA	SLSDC	STB
Business Continuity and Disaster Recovery Plan (BCDRP) did not exist.	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 exercises tested and failed.	X		X				X		X	X	X		X
Contingency plans not tested.	X		X	X				X	X		X		X
Contingency test results not reported.	X	X	X	X				X	X		X		X
No evidence of system backup at alternative processing sites.	X		X	X					X		X		X
System backup not in accordance with procedures.	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
No evidence of risk assessment performed for alternative processing sites.	X	X	X			X		X		X	X		X

Source: OIG Analysis

[a] The deficiency described was found in one or more OA's sample systems that OIG assessed.

Based on these results, we estimate that OAs did not complete contingency testing for 202 of DOT's 420 systems.[25] Without proper C&A, serious system weaknesses may remain unidentified. Consequently, the Department cannot ensure that its systems are reasonably protected against security threats. Furthermore, a lack of complete contingency testing means that OAs may not be able to recover their systems from unplanned shutdowns in time to minimize business disruption.

DOT Does Not Coordinate the Use of Shared System Security Controls

NIST requires providers of common controls—security controls that support multiple information systems—to have policies and procedures for their use, document the controls in a separate security plan, conduct a C&A of the common controls, monitor their effectiveness, and inform users when changes occur that

[25] Our estimate has a margin of error of +/-51 or 12.2 percent at the 90 percent level of confidence.

may adversely affect the protections provided by or expected of these controls. NIST also requires that the senior information security officer for the organization coordinate with common control providers to ensure that the required controls are developed, implemented, and assessed for effectiveness. However, DOT does not have common control procedures. Furthermore, DOT providers do not have a security plan or a formal process to advise users when the common controls are not effective or in place. In addition, system managers who use inherited controls—a control that is part of a network and used by a software application that resides on the network—frequently do not verify the functionality of the control as part of their system accreditation process. Finally, there is no coordination to ensure that the controls are effective. All 13 OAs used common controls as part of their system C&As, but none had a documented process for the use of the common controls or had verified the functionality of inherited controls.

The lack of adequate management of common controls results in numerous systems that have been accredited while relying on missing controls and hence are operating at an unacceptable level of risk.

DOT's Continuous Monitoring of Security Controls Remains Ineffective

OMB guidance calls for agencies to develop strategies for the continuous monitoring of security control effectiveness. DOT has deferred implementation of continuous monitoring to the OAs; however, as in previous years, the Department's continuous monitoring policy and procedures were not sufficiently detailed to ensure OAs comply with OMB's guidance. For example:

- Four of the 13 OAs—FAA, MARAD, OIG, and OST—continuous monitoring policies and procedures are still in draft form. FHWA and FMCSA have plans, but have not begun to develop continuous monitoring policies and procedures. RITA, SLSDC, and STB either did not have or did not provide documentation that addressed continuous monitoring policies and procedures.
- FAA, FHWA, FMCSA, MARAD, NHTSA, OST, RITA, SLSDC and STB reported that they annually assess selected security controls but do not perform continuous monitoring.
- Thirty sample systems failed our reviews of continuous monitoring processes. These systems are at FAA, FHWA, FMCSA, FTA, MARAD, OST, RITA, SLSDC, and STB.

The Department's lack of guidance on continuous control monitoring diminishes the OAs' abilities to monitor their systems' security, and to respond quickly to new threats. To address these weaknesses, OCIO has informed us that it recently acquired a highly complex software solution, which they are piloting. If properly

implemented, this software will allow management to rapidly remediate weaknesses and protect systems, and instantaneously report on security status.

OAs Do Not Designate All Contractor-Operated Systems in Accordance with OMB Guidance

OMB also requires agencies to maintain up-to-date inventories of their information systems.[26] These inventories must designate each system as either "contractor operated" or "organization operated," based on who manages the system—the Federal agency or an outside entity. Specifically, contractor operated systems are those that are either fully or partially owned or operated by another agency, a contractor, or other entity. For fiscal year 2012, OCIO provided OAs new guidance[27] that includes this definition of contractor operated. However, OAs are not designating all their systems in accordance with the guidance. We determined that 24 of the 60 systems were contractor systems, but only 4 were designated as such.

Because contractors or other entities, rather than the OAs, manage the security controls in contractor operated systems, the systems represent higher risk to the Department. The lack of an accurate inventory of these systems makes it difficult for the Department to know which systems it is not managing and consequently pose higher risk.

DOT Lacks a Secure Remote Access Management Program

OMB and NIST provide guidance for agencies on controlling remote access to their systems, and DOT has incorporated the guidance into its policy. DOT OCIO policy on remote access delegates responsibility to OAs for documenting, managing, and controlling remote access of the systems under their control.[28] However, the OAs' remote access controls do not comply with DOT's policies and guidance. For example:

- COE, STB, and Volpe do not require the use of multifactor authentication.
- COE, Volpe, FMCSA field sites, and STB do not fully comply with NIST guidance for authorizing, monitoring, and controlling remote access.
- STB reported it has not established a process for securing and monitoring remote devices.

---

[26] OMB defines "contractor system" as any system fully or partially provided or managed by another agency, contractor, or other source.

[27] *DOT FISMA Inventory Guide*, 6 June 2012.

[28] Remote access management to DOT information and information systems is separated among 7 entities; COE, FMCSA for field sites, OIG, STB, Volpe, USMMA, and FAA. COE manages remote access for these OAs with exception of STB and FMCSA field sites.

Without effective controls over remote access, DOT cannot ensure that only authorized computers and personnel access its information systems or minimize risks of malware on its networks or loss of sensitive information.

DOT Has Not Fully Implemented Use of Personal Identity Verification Cards for Multifactor User Identity Authentication for System Access

OMB required that, by 2012, all Federal personnel use personal identify verification (PIV) cards to log on to agency computers for multifactor user identity authentication. In a briefing to the CIO Council in December 2011, the Department indicated that it would require PIV card login for 75 percent of desktop and laptop users by September 30, 2012. However, as of June 2012, only 42 percent of DOT's systems are enabled for user logon with PIVs, and only 7 percent of the Department's systems require the use of PIV for user identity authentication. Because DOT does not fully employ multi-factor authentication for computer users, it is unable to adequately authenticate the identities of all users.

DOT's Account Management Program Remains Incomplete

While the Department is working to resolve the account management issues we identified in our 2011 report, its account management controls still do not meet DOT and NIST policies and guidance, exposing DOT to increased risk of unauthorized access to information systems. For example:

- The Department does not adequately distinguish between user and non-user accounts, as required by NIST. Proper identification of accounts is essential to prevent non-user accounts from being used to gain unauthorized access to the systems.
- The Department does not disable inactive accounts within the departmentally mandated time frame of 60 days.

DOT CONTINUES TO LACK AN EFFECTIVE PROCESS FOR THE REMEDIATION OF SECURITY WEAKNESSES

FISMA requires agencies to develop a process to remediate information security weaknesses. OMB similarly requires departments to develop POA&Ms for detected system weaknesses and to prioritize remediation based on the seriousness of each weakness. OAs designate weaknesses as high, medium, or low priority for remediation.

However, the Department has not improved its management of information security weaknesses. Of the 5,265 open POA&Ms, 2,161 were past their due dates for resolution, including 432 that are over a year overdue. These numbers represent a 7 percentage points increase in incomplete POA&Ms over 2011. We also found that 132 of these open POA&Ms have no completion dates (see Table 8).

Table 8: DOT's Open POA&Ms and Days Overdue, as of July 31, 2012

OA	Number of Open POA&Ms	Days Overdue					Summary of Timeliness Issues		
		1–60	61–90	91-120	121–365	366+	No due date	Total overdue, current	Total overdue, expected
COE	7	1	0	2	0	4	0	7	0
FAA	4,397	400	122	99	510	329	20	1,480	2,917
FHWA	25	6	0	0	1	0	0	7	18
FMCSA	298	130	0	0	79	0	82	291	7
FRA	26	6	0	0	0	19	1	26	0
FTA	30	0	0	0	12	1	0	13	17
MARAD	169	98	0	4	44	0	0	146	23
NHTSA	0	0	0	0	0	0	0	0	0
OIG	13	0	0	0	0	13	0	13	0
OST	118	24	0	0	43	4	0	71	47
PHMSA	39	9	0	0	0	0	26	35	4
RITA	32	0	0	0	0	10	1	11	21
SLSDC	3	1	0	0	0	0	0	1	2
STB	108	5	0	0	1	52	2	60	48
Total	**5,265**	**680**	**122**	**105**	**690**	**432**	**132**	**2,161**	**3,104**

Source*:* DOT Open POA&Ms in Cyber Security Assessment and Management (CSAM) system

Departmental policy requires OAs to record all known weaknesses in the Department's CSAM database—a repository meant to facilitate tracking of security weaknesses and their remediation. However, we found that 18 of our 60 sample systems had POA&Ms that OAs had not recorded in CSAM. Based on these results, we estimate that 96 systems out of 420[29] did not have all known POA&Ms recorded in CSAM.

Finally, OMB guidance calls for CIOs to meet with their OAs quarterly to review progress on POA&M completion. From the evidence OCIO provided us, it only

[29] Our estimate has a margin of error of +/-39 systems or 9.2 percent at the 90 percent level of confidence.

met with OAs in September 2012, not quarterly. Completing POA&Ms in a timely manner is critical to ensuring that systems are adequately secured and protected because weaknesses that are unresolved for extended periods of time create the risk of exploitation.

CONCLUSION

Protecting DOT's information systems is critical for ensuring the Nation's transportation systems run smoothly and safely and Federal dollars for major programs are used efficiently and appropriately. While DOT has finalized its information security policy and initiated a number of initiatives to enhance it cyber security program, persistent control weaknesses continue to put at risk the confidentiality, integrity, and availability of the Department's information. These weaknesses, many of which are longstanding, also render DOT vulnerable to hackers and others who continue to aggressively probe and compromise Federal networks. Until DOT takes additional actions to correct these weaknesses and comply with Federal requirements, it will continue to expose its IT systems 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 Acting Chief Information Officer take the following actions in addition to 21 recommendations that are still open from prior FISMA reports:

Information Security Policy

1. Work with Operating Administrations to enhance and develop their internal procedures for inheriting controls, continuous monitoring, and capital planning to better address key NIST requirements.

Enterprise-Level Weaknesses

2. Establish timeframes for incident remediation based on risk.
3. 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. Develop, document and approve an enterprise-wide risk management program and strategy as defined by NIST 800-39.

Information System Security

5. 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.

AGENCY COMMENTS AND OIG RESPONSE

A draft of this report was provided to the Department's Acting CIO on November 1, 2012. On November 13, 2012, we received the Department's response, which can be found in its entirety in the Appendix. In its response, the Department highlighted the progress it made during fiscal year 2012 to improve its cyber security. In addition, the Department outlined its priorities for fiscal year 2013, and committed to providing us with specific planned actions and milestones to address our recommendations.

ACTIONS REQUIRED

In accordance with Department of Transportation Order 8000.1C, we would appreciate receiving your detailed action plans and target dates for the recommendations in this report within 30 calendar days. We will review the Acting Chief Information Officer's detailed action plans when provided to determine whether they satisfy the intent of our recommendations. All corrections are subject to follow-up provisions in DOT Order 8000.1.C. We appreciate the courtesies and cooperation of the CIO Office and the Operating Administrations' 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

The Federal Information Security Management Act of 2002 (FISMA) requires us to perform an independent evaluation to determine the effectiveness of the Department's information security program and practices. FISMA further requires that our evaluation include testing of a representative subset of systems and an assessment, based on our testing, of the Department's compliance with FISMA and applicable requirements. On February 15, 2012, the Department of Homeland Security (DHS) issued FISM 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which provides instructions to Inspectors General for the completion of their FISMA evaluations and the required DHS template.

To meet FISMA and OMB requirements, we selected a representative subset of 58 of 420 departmental systems (see Table 9 below) 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. To evaluate USGCB/FDCC compliance within the Department, we selected a stratified sample of 1,257 out of 82,963 devices to be scanned for compliance. We created a script to extract the test results of FDCC/USGCB controls from 340 out of 1,257 devices that were available for scanning.

We evaluated prior year recommendations and supporting evidence to determine what progress if any was made in the areas of continuous monitoring, configuration management, risk management, security training, contractor services, and identity and account management. In addition, we also conducted testing to assess the Department's inventory, its overall process for resolution of information security weaknesses, configuration management, incident reporting, security-awareness training, remote access, security capital planning, and account and identity management. Our tests included analysis of data contained in the Department's CSAM system, reviews of supporting documentation, and interviews with departmental officials. We conducted this audit between February and October 2012 in accordance with generally accepted Government auditing standards. As agreed to with the Department our FISMA review covered through year-ending July 31, 2012.

Table 9: OIG's Representative Subset of DOT Systems, by OA

No.	System	Impact Level	Contractor System? [a]
Federal Aviation Administration			
1	Whistleblower Protection Program	High	No
2	Inspector Credentials	High	No
3	Web Operations Safety System	High	No
4	Facility Safety Assessment System-ATO	Low	No
5	Bandwidth Manager	Moderate	No
6	AST Local Area Network	Moderate	No
7	Air Route Surveillance Radar Model 4	Moderate	No
8	Aircraft Certification Office Subsystem	Moderate	No
9	Safety Management Information System	Moderate	No
10	Interim Voice Switch Replacement System	Moderate	No
11	Advanced Qualification Program	Low	No
12	Obstruction Evaluation/Airport Airspace Analysis	Low	No
13	Safety Issues Reporting System	Moderate	No
14	Monitor Safety Analyze Data	Moderate	No
15	FAA Read-Only Data Interface	Moderate	Yes
16	Real Estate Management System	Moderate	No
17	ESC Department of Commerce Infrastructure	Moderate	No
18	ATO Application Portal	Moderate	No
19	Messaging Services	Moderate	No
20	Data Multiplexing Network	Moderate	No
21	Technical Support Services Contract- Work Release Information Tracking System	Low	No
22	Enhanced Terminal Voice Switch	Moderate	No
Federal Highway Administration			
23	Rapid Approval & State Payment System	High	No
24	ITD Application and Oracle Database Servers	High	No
25	FHWA Organization Information System	Moderate	No
26	Motor Fuels and Finance Analysis System – Highways	Low	No
27	Federal Lands Labor Cost Distribution Process	Low	No
Federal Motor Carrier Safety Administration			
28	CDLIS-Gateway	Moderate	Yes
29	Hazardous Material Package Inspection Program	Moderate	No
30	Performance and Registration Information Systems Management	Low	No
Federal Railroad Administration			
31	Track Research Instrumentation Platform Information System	Moderate	Yes
32	Locomotive Engineer Training Simulator	NC	No

No.	System	Impact Level	Contractor System? [a]
Federal Transit Administration			
33	TEAM	Moderate	No
34	FTA Inter/Intranet	Moderate	No
Maritime Administration			
35	Maritime Service Compliance System	Moderate	No
36	Electronic Invoice System	Moderate	No
37	FOIAXpress	Low	Yes
National Highway Traffic Safety Administration			
38	EDS	Moderate	No
39	Artemis	Moderate	No
Office of Inspector General			
40	US DOT/OIG Infrastructure	Moderate	No
41	US DOT/OIG TIGR System	Moderate	No
Office of the Secretary of Transportation			
42	Drug and Alcohol Testing Management Information System	Moderate	No
43	Facilities and Building Management System	Moderate	No
44	Web Printing System	Moderate	No
45	CASTLE	Moderate	No
46	Cyber Security Assessment and Management	High	No
47	Security Operations Systems	High	No
Pipelines and Hazardous Materials Safety Administration			
48	Hazardous Materials Information System	Moderate	No
49	PHMSA Portal System	Moderate	No
Research and Innovative Technology Administration			
50	RITA Mission Support	Low	No
51	IEC Data Warehouse	Moderate	No
52	Transtats	High	No
53	Airline Reporting Data Information System	High	No
Saint Lawrence Seaway Development Corporation			
54	Financial Management System	Low	No
Surface Transportation Board[b]			
55	Case Management System	Moderate	No
56	Local Area Network	Moderate	No
Common Operating Environment			
57	Common Operating Environment	High	No
58	Business Communications System	Moderate	No

Source: OIG

[a] DOT Cyber security Definition of Contractor System

[b] For purpose of this report, STB were selected as part of the sample. Exhibit C defines STB obligation to comply with DOT requirements.

Exhibit A: Scope and Methodology

As required, we submitted to OMB qualitative assessments pertaining to DOT's information security program and practices. In addition to the preparation of our submission, we reviewed the Department's progress in resolution of weaknesses and implementation of recommendations identified in our prior FISMA reports.

We performed our information security review work between February 2012 and October 2012. We conducted our work at departmental and OA Headquarters' offices in the 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 require us to disclose impairments of independence or any appearance thereof. OMB requires that the FISMA template include information from all DOT OAs, including OIG. Because the OIG is a small component of the Department, based on number of systems, any testing pertaining to the OIG or its systems does not impair our ability to conduct this mandated audit.

Previous audit reports on the Department's information security program issued in response to FISMA's mandate include the following:

- *Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information Systems*, FI-2012-007, November 14, 2011
- *Timely Actions Needed to Improve DOT's Cybersecurity*, FI-2011-022, November 15, 2010
- *Audit of DOT's Information Security Program and Practices*, FI-2010-023, November 18, 2009
- *DOT Information Security Program*, FI-2009-003, October 8, 2008
- *DOT Information Security Program*, FI-2008-001, October 10, 2007
- *DOT Information Security Program*, FI-2007-002, October 23, 2006
- *DOT Information Security Program*, FI-2006-002, October 7, 2005
- *DOT Information Security Program*, FI-2005-001, October 1, 2004
- *DOT Information Security Program*, FI-2003-086, September 25, 2003
- *DOT Information Security Program*, FI-2002-115, September 27, 2002
- *DOT Information Security Program*, FI-2001-090, September 7, 2001

EXHIBIT B. Status of Prior Year's Recommendations

Table 10: OIG Recommendations for Fiscal Year 2011, and Their Status

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.
2	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.
3	Open	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.
4	Closed	In conjunction with OA CIOs, verify that backup media are properly secured and regularly tested.
5	Open	In conjunction with OA CIOs, verify that minimum security controls are adequately tested for deficient systems.

Table 11: OIG Recommendations for Fiscal Year 2010, and Their Status

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.

No.	Status	Recommendation
4	Open	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.
6	Open	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	Open	Conduct periodic tests to assess FDCC compliance and deployment of patches, including service packs.
9	Open	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	Open	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	Open	Research and standardize automated tools that will proactively monitor remote devices connecting to DOT networks.
21	Open	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 12: OIG Recommendations for Fiscal Year 2009, and Their Status

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	Open	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	Close	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	Open	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	Open	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 OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Table 13: OA System Inventory Counts for Fiscal Years 2012 and 2011

	Fiscal Year	
Organization[a]	**2012**	**2011**
Federal Aviation Administration (FAA)	283	297
Federal Highway Administration (FHWA)	21	21
Federal Motor Carrier Safety Administration (FMCSA)	18	18
Federal Railroad Administration (FRA)	14	13
Federal Transit Administration (FTA)	5	5
Maritime Administration (MARAD)	20	25
National Highway Traffic Safety Administration (NHTSA)	10	11
Office of Inspector General (OIG)	2	2
Office of the Secretary (OST)[b]	30	31
Pipeline and Hazardous Materials Safety Administration (PHMSA)	7	5
Research and Innovative Technology Administration (RITA)	15	14
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)[c]	2	2
Total Systems	**428**	**445**

Source: OIG, and DOT CSAM as of August 6, 2010

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

[b.] For purposes of reporting under FISMA COE systems are counted under Office of the Secretary.

[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. 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
Gerald Steere	Supervisory Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Tracy Colligan	Information Technology Specialist
Jenelle Morris	Information Technology Specialist
Jason Mott	Information Technology Specialist
James Mullen	Information Technology Specialist
Mitch Balakit	Information Technology Specialist
Nileshkumar Patel	Information Technology Specialist
LaKarla Lindsay	Referencer
Petra Swartzlander	Senior Statistician
Megha P. Joshipura	Statistician
Karen Sloan	Communications Analyst
Susan Neill	Writer-Editor

APPENDIX. AGENCY COMMENTS

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

Memorandum

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

Date: November 9, 2012

From: Tim Schmidt
Acting DOT Chief Information Officer

Reply to Attn. of:

To: Calvin L. Scovel III
Inspector General

DOT Made Significant Progress on Cybersecurity Priorities in 2012

Last year, the Administration set cross-agency priority goals for cybersecurity aimed at improving the overall security posture of Federal computer networks through the implementation of key cybersecurity capabilities within each agency. The Department of Transportation (DOT) established those goals as a priority this past year, and has made significant progress, while also developing DOT initiatives focused on achieving the greatest potential cybersecurity benefit to the agency. The Department continues to improve its cybersecurity posture while it simultaneously maintains critical operational systems and responds to a significant number of new information technology requirements set by the Office of Management and Budget (OMB). Key cybersecurity accomplishments over the past year include:

- **Continuous Monitoring** — DOT deployed an automated enterprise continuous monitoring solution that addresses DHS required capabilities across nine (9) operating administrations (OAs) and more than 11,500 computers. The system is scalable to cover all of DOT. Results to date demonstrate greater than 94% compliance with government configuration standards for our Microsoft Operating Environment.

- **PIV Card Expansion** — The DOT PIV card program includes more than 95% of DOT Federal and contract personnel. More than 34% of those personnel also now have the capability to use the PIV cards for secure login to DOT systems.

- **Enhanced System Security** — DOT implemented a solution to require the PIV card for authentication to DOT's multi-function printer fleet, while the Federal Highways and Maritime Administrations, and the Office of the Secretary have enabled use of the PIV card to access mission systems within their organizations.

- **Improved Telework Security** — DOT implemented a scalable virtual desktop infrastructure (VDI) solution for up to 1,500 personnel to provide Federally-compliant secure remote access to DOT systems and information.

- **Revised IT Governance Structure** — The Department issued a revised governance policy, which reinvigorates Information Technology governance within DOT, and provides for integration of cybersecurity and enterprise architecture into agency decision-making while providing a risk management framework.

DOT Cybersecurity Priorities for FY 2013

DOT has established cybersecurity priorities for FY2013 to ensure that the most effective possible use is made of increasingly constrained resources and to identify clear direction to contend with the many competing priorities for these resources. While acting upon issues identified in the OIG draft report are important to FISMA objectives, it is essential that we focus on the highest priority actions in order to achieve meaningful progress in improving the Department's cybersecurity posture. As a result, addressing some of the OIG draft report issues may require more than a single year.

DOT's Cybersecurity Priorities for FY 2013 include:

- **Federal Cybersecurity Requirements** — Continued implementation of the Administration's cybersecurity requirements for continuous monitoring, strong authentication via the PIV card, and full implementation of the Trusted Internet Connection program.

- **Enhanced Risk Management and Continuous Monitoring** — Increased application of the DOT risk management and continuous monitoring programs, and collaboration with DHS to develop and implement the next iteration of the Federal continuous diagnostics and monitoring program.

- **Secure Departmental E-mail in the Cloud** — DOT will migrate e-mail and collaboration tools to the cloud, resulting in improved resilience and security, both through enhanced capabilities of the cloud provider's systems, and by driving changes within DOT to consolidate, and standardize portions of its IT infrastructure in preparation for the migration.

- **IT Governance Implementation** — DOT will implement its IT governance program, to include both risk management and enterprise architecture, in a manner intended to provide useful information for making informed and appropriate decisions on IT investments.

DOT Using All Available Resources to Identify Threats and Manage Risk

The cybersecurity challenges that threaten the viability of the Department's information technology systems continue to evolve and have grown significantly more sophisticated. The

Department must make effective use of all resources available, including the OIG's annual FISMA review, to identify threats to systems, and prioritize actions to address those threats. The priorities identified in this memo factor consideration of the OIG's work, Governmentwide 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.

We appreciate the positive interactions with the OIG staff through the duration of this review. We intend to provide, under separate cover, a specific response to each recommendation identifying actions planned and anticipated milestones. Please contact Andrew Orndorff (andrew.orndorff@dot.gov, 202.366.7111) in the Office of the Chief Information Officer with any questions."