Office of Inspector General

Audit Report

FISMA 2011: PERSISTENT WEAKNESSES IN DOT'S CONTROLS CHALLENGE THE PROTECTION AND SECURITY OF ITS INFORMATION SYSTEMS

Department of Transportation

Report Number: FI-2012-007
Date Issued: November 14, 2011

Memorandum

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

Subject: ACTION: FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information Systems Department of Transportation Report Number: FI-2012-007

Date: November 14, 2011

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 400 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 information technology (IT) investments among Federal civilian agencies. The Department's financial systems manage and disburse approximately $90 billion in Federal funds annually. During 2011 alone, computer hackers have placed a number of major entities' IT systems at risk, including those at the Central Intelligence Agency and Google.

To protect the information systems that support Federal operations from cyber threats, the Federal Information Security Management Act (FISMA) of 2002 requires agencies to develop, document, and implement agencywide 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 127 security metrics 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

[1] For purposes of this report, enterprise-level controls are those controls that should be implemented Department-wide—security training, incident response and reporting, capital planning and investment control, and configuration management—and are generally not system-specific.

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

To conduct our audit and address OMB's 127 metrics, we tested a statistical sample of 64 out of 445 systems, performed analytical reviews of data contained in the Department's Cyber Security Assessment and Management system (CSAM), tested user accounts in 19 general support systems, reviewed supporting documentation, and interviewed departmental officials. We conducted this audit between February and October 2011 in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology.

RESULTS IN BRIEF

Despite improvements the Department made to its security controls over the past year, its information security program does not meet Federal requirements and is still not as effective as it should be. Furthermore, the Department has successfully addressed only 19 of the 25 recommendations that remained open since November 2009, and 6 of the 27 recommendations we made in our last FISMA report, issued in November 2010. Following are details of our findings.

1. The Office of the Chief Information Officer (OCIO) has not developed the required procedural guidance to augment its high-level security policy in order for Operating Administrations (OA) to manage information security effectively. OCIO focused its efforts on revising its existing policy and created a strong and flexible cybersecurity policy for the Department, except for the Office of the Secretary of Transportation (OST). According to OCIO, OST management had differing views on needed policy changes. Because agreement was not reached, OST, which includes the Common Operating Environment[3] (COE), is operating without a cybersecurity policy. These weaknesses in OCIO's policy and procedures contribute to the other issues we identified.

2. The Department has not made sufficient progress to implement enterprise-level controls. While the Cyber Security Management Center (CSMC) implemented controls that enabled it to confirm that it reported all major security incidents that it received to the Department of Homeland Security (DHS), other weaknesses persist. For example, DOT is still unable to effectively track how many contractors it has on board or manage security baseline configurations for all of its systems. Although more OAs have tools

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

[3] COE provides network infrastructure support to DOT's Headquarters and remote offices, except FAA and Federal Motor Carrier Safety Administration field sites.

to assess compliance with Federal Desktop Core Configuration (FDCC)[4] requirements, which prescribe secure settings for Windows Experience (XP) software, DOT's compliance has dramatically declined from 90 percent to 70 percent since our last review. Furthermore, the Department does not have any controls that ensure information security is incorporated in its capital planning and investment process.

3. DOT has not established adequate controls to protect its systems or to recover them in the event of a disruption. While the completeness of certification and accreditation (C&A) documents has improved, significant weaknesses in the C&A process remain. For example, we project that for 239 of its 445[5] systems, or 54 percent, the Department did not properly test the minimum security controls required by the National Institute of Standards and Technology (NIST). We also found than half of the systems in our sample had missing or incomplete contingency plans for system recovery in case of disruptions, and over 40 percent of critical systems did not have adequate backup facilities or testing of their contingency plans. The Department also lacked adequate controls over continuous monitoring of system security, oversight of contractor-operated systems and their security, and remote access and account management. For example, the Department does not use two-factor authentication to secure remote access to its systems, and we identified network accounts assigned to individuals no longer employed by DOT.

4. DOT has not effectively identified, tracked, or prioritized information security weaknesses in plans of action and milestones (POA&M) to efficiently resolve these weaknesses. The Department tracked approximately 4,700 system weaknesses but did not remediate over a third of them within approved timeframes—a slip in performance compared to last year.

Together, these weaknesses significantly increase the risk that systems will become victim to cyber attacks or disruptions that can compromise the integrity, availability, and confidentiality of data needed to fulfill DOT's missions.

We are making a series of recommendations to assist the Department in the establishment and maintenance of an effective information security program—one that complies with FISMA, OMB, and NIST requirements. Exhibit C identifies the recommendations from our two prior reports that the Department still needs to resolve.

---

[4] FDCC are security configuration settings developed by the National Institute of Standards and Technology (NIST), the Department of Defense, and the Department of Homeland Security (DHS) for certain Windows operating systems, including XP. OMB has mandated agencies to adopt these settings.

[5] Our estimate is has a margin of error of +/- 9.1 percent, and 90 percent level of confidence.

BACKGROUND

A secure global digital information and communications infrastructure is one of the President's seven guiding principles in the protection of the American people.[6] As the White House has reported, both the Federal Government and the private sector face cybersecurity threats, including terrorists and international crime groups that target U.S. citizens, commerce, critical infrastructure, and the Government with attempts to compromise computer-based information. Undeterred, these individuals could undermine national security and degrade civil liberties.

FISMA requires each Federal agency to develop, document, and implement an agencywide program to secure the information and information systems that support the operations of the agency, including those provided or managed by another agency, contractor, or other source. 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. In support of and reinforcing this legislation, OMB, through Circular A-130, Appendix III*, Security of Federal Automated Information Resources*, requires executive agencies within the Federal Government to plan for security, ensure that appropriate officials are assigned security responsibility, periodically review the security controls in their information systems, and authorize system processing prior to operations and periodically thereafter.

DOT tracks its 445 information systems by 13 components. Exhibit B lists the 13 components and their respective number of systems. For purposes of reporting under FISMA, we consider "operating administrations" to include all 13 components.

Since 2001, we have reported on weaknesses in DOT's information security program and practices. Our three most recent reports noted the following.

- In October 2008, we reported that the Department's information security program and practices were not effective.[7] Specifically, DOT had not established adequate policies, procedures, and training to identify weaknesses in information security and protect computer systems and networks, including those containing personally identifiable information (PII), or recover them should an incident occur. We made 27 specific recommendations to address these deficiencies.

- In November 2009, we reported that DOT had issued its information security policy—the first step in the development of a sustainable information security

[6] White House Issues: Homeland Security (www.whitehouse.gov/issues/homeland-security).
[7] *DOT Information Security Program*, FI-2009-003, October 8, 2008.

program—and improved the COE's FDCC compliance.[8] However, the Department had not made sufficient progress in other areas. Its information security program did not meet all Federal requirements and was not as effective as it should have been. We made 27 additional recommendations to correct critical vulnerabilities and assist DOT in the establishment of a more mature information security program.

- In 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.[9] The Department's information security system was still not effective. In its assurance letter to the President, the Department reported that its compliance with FISMA during 2010 constituted a material weakness in internal controls.

For 2011, OMB added one additional reporting area for IGs audits—Capital Planning and Investment Control—and increased the number of metrics in the other 10 reporting areas. The 127 metrics for IGs' 2011's review represents a 20 percent increase over the prior year. OMB also changed the "certification and accreditation" reporting area to "risk management" to align with NIST's 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, dated February 2010.

DESPITE IMPROVEMENTS, DOT'S INFORMATION SECURITY POLICY AND PROCEDURES REMAIN INADEQUATE

Although it has made improvements, the Department's information security policy and procedures are still inadequate. FISMA requires each Department's Chief Information Officer to develop and maintain information security policies, procedures, and control techniques to address security requirements. In prior reports, we recommended revisions to the Department's policies that direct its OAs' security efforts. In June 2011, OCIO issued a strong and flexible cybersecurity policy for the Department. However, according to OCIO, OST management had differing views on needed policy changes. Because agreement was not reached, OST, which includes the Common Operating Environment (COE), is operating without cybersecurity policy. Furthermore, as stated in our prior three reports, the OAs have limited or no procedural guidance from OCIO to instruct them on how to effectively and consistently implement information security. Table 1 details the deficiencies in the Department's policy and procedures.

---

[8] *Audit of DOT's Information Security Program and Practices,* OIG Report FI-2010-023, November 18, 2009.
[9] *Timely Actions Needed to Improve DOT's Cybersecurity*, OIG Report FI-2011-022, November 15, 2010.

Table 1: Deficiencies in Policy and Procedures

FISMA Security Program Area	Office of Inspector General's (OIG) Evaluation
Certification and Accreditation (C&A) of Controls	
The assessment of security controls to determine if the controls have been implemented effectively.	C&A procedures remain in draft form.
Continuous Monitoring of Controls	
Required as part of the security authorization process to ensure that controls remain effective over time.	Procedures are not sufficiently detailed to guide Agency personnel in the development of practices for the monitoring of their systems.
Plans of Action and Milestones (POA&M)	
Tracks the measures implemented to correct security weaknesses and eliminate vulnerabilities.	Revised policy references procedural guidance that remains in draft form.
Security Awareness and Specialized Training	
Annual training required by FISMA for Government and contractor personnel.	Policy does not require all Government and contractor personnel—those who use information systems as well as those who do not—to receive training, and procedures are not sufficiently developed to guide OAs in identification, tracking and validation of contractors that require annual security training.
Capital Planning and Investment Control	
Policy and procedures that ensure that security funding is incorporated in system life-cycles.	The policy and procedures for management of security costs as part of IT capital planning are not developed.
Account and Identity Management	
Controls for management and monitoring of network accounts.	The procedures are not sufficiently developed to guide OAs in establishment of controls. For example, procedures do not fully address conditions for group memberships, approval processes, conditions required to grant access, and temporary accounts, among other things.
Configuration Management	
Policy and procedures that ensure that all system owners have implemented approved security control baselines.	Does not include detailed procedural guidance for management of policy requirements. For example, there is little guidance on the adoption of hardware and software security baselines.
Contractor Oversight	

FISMA Security Program Area	Office of Inspector General's (OIG) Evaluation
Monitoring of the effectiveness of support system security provided or managed by contractors, or other agencies or sources.	Policies and procedures do not include an OMB-compliant definition of "contractor system."
Remote Access	
Components for telework and remote access, including client devices, servers, and internal resources, should be secured against known possible weaknesses, including the lack of controls for physical security, the use of unsecured networks, connections between infected devices and internal networks, and the availability of internal resources to external hosts.	Procedures do not establish an effective approach to identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications.

Source: OIG Analysis

The lack of adequate Departmentwide guidance on security requirements creates a possibility that OAs will develop internal procedures and practices that may not comply with OMB or DOT's requirements, and has contributed to the other weaknesses documented in this report.

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

DOT's Departmentwide controls—those that must be implemented at the enterprise level—are still inadequate to ensure its contractors receive the required security training, security incidents are detected and reported, configuration baselines are appropriately managed, and 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[10] are adequately trained in their security responsibilities before they are allowed access to agency information systems. Furthermore, both FISMA and OMB require agencies to provide basic security awareness training to employees and contractors that never access computer systems as well as to those who do. However, as we have previously reported, the Department lacks a system that effectively tracks all contractors working for the Department, and therefore cannot determine whether its contractors have received required training. Further, because DOT policy requires its CIOs only to ensure that all users of DOT's information system

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

receive training, many non-users, who frequently are contractors, do not receive training or are not accounted for.

For 2011, DOT attempted to establish a baseline number of contractor personnel by using a list of currently employed contractors extracted from its Personal Identity and Verification Badge System. However, the Department had no way to confirm that all employed contractors were included in the baseline. Moreover, in contrast to FISMA and OMB policy, [11] it removed from the list contractors that did not appear to have access to IT systems because of the services they provide, such as security guards and janitorial. Contractor tracking issues represent significant security risks to the Department because personnel without security awareness training are more likely to become victims of social engineering or commit acts that compromise information security.

The Department's Incident Reporting Process Does Not Monitor All DOT Networks

DOT has instituted controls to improve reporting of intrusion incidents, but does not monitor all of its networks for intrusion. OMB policy requires departments to report several categories of security incidents to DHS's U.S. Computer Emergency Readiness Team (US-CERT). Last year, we found that DOT's reporting process did not ensure that all of the required incidents were reported to US-CERT.

Since then, FAA's CSMC has instituted new controls that provide reasonable assurance that all incidents it receives from OAs get reported to US-CERT. However, CSMC does not monitor all DOT networks. For example, because CSMC does not monitor the United States Merchant Marine Academy's (USMMA) network, it does not receive any intrusion detection reports from the Academy. Furthermore, CSMC monitors only two of the National Airspace System's (NAS) many systems. Because it cannot be sure that all incidents are discovered, the Department risks cyber attacks going undetected and unaddressed.

The Department Has Not Fully Met 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. However, we found deficiencies in DOT's compliance with FDCC settings, and incomplete implementations of other configuration standards

[11] OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

throughout the Department. Inadequately configured software also increases security vulnerabilities that could impact DOT's mission and business operations.

OAs Are Not in Compliance With FDCC Requirements

OMB requires agencies that have deployed certain software, such as the Windows XP operating system, to adopt FDCC security configurations settings. OMB also requires departments to meet all NIST configuration settings in order for them to be 100 percent compliant with configuration standards. We drew a statistical sample of 903 out of 90,169 OA computers for the OAs to scan for compliance with controls; they scanned 437 systems but the other 466 were not operating or were otherwise unavailable.[12] We estimate that 70 percent[13] of controls are compliant with FDCC requirements, a decline of approximately 20 percentage points from 2010. None of the computers tested was fully compliant with NIST settings. Table 2 shows the total controls tested and passed.

Table 2: FDCC Sample Test Results of Controls for Windows Operating System at OAs

OA	Tested	Passed	% Passed
FAA	119,984	74,513	62.10%
Federal Motor Carrier Safety Administration (FMCSA)	7,788	5,511	70.76%
COE[a]	15,171	11,040	72.77%
Surface Transportation Board (STB)	20,856	9,928	47.60%
John A. Volpe National Transportation Systems Center (Volpe)	15,806	11,347	71.79%
USMMA	8,547	5,232	61.21%
OIG[b]			
Department Totals[c]	**188,152**	**117,571**	**62.49%**

Source: OIG

[a]The Department consolidated OAs' network infrastructures (email, desktop computing, and local area networks) into a common IT infrastructure.

[b] On July 22, 2011, OIG informed us that it did not use Security Content Automation Protocol tools. After the conclusion of our fieldwork, OIG informed us that it did for FDCC.

[c] Totals may not add due to rounding.

We also noted the following areas in which DOT did not comply with FDCC requirements.

[12] Scanning tools test only computers that are operating during a scan. Other routine factors can contribute to a scanning tools inability to test a specific computer.

[13] The estimate has a margin of error of +/-11.5 percentage points at the 90% confidence level.

- One of the Department's controls for the use of approved configuration settings is the application of uniform approved settings at all workstations. However, numerous settings that should have been identical at all workstations were different. For example, FMCSA had almost 30 different settings among its computers. We did not determine the cause for the variations in settings, but such differences can be caused by malware or viruses.

- OMB requires agencies to use Security Content Automation Protocol[14] (SCAP)-validated tools to certify that their systems comply with FDCC and United States Government Configuration Baseline (USGCB) standards. Once agencies have deployed these standard configurations to personnel's computers, they are required to monitor and manage the configurations to ensure they are not modified. Three OAs either had less than 100 percent standard configurations deployed on their systems or did not provide evidence of total deployment. For example, OIG did not use SCAP tools to ensure compliance for its systems.

- Agencies may create deviations from control settings when it determines that the settings impact operations, such as the running of legacy applications. However, if an OA opts to create such deviations, the OCIO must review and approve them to prevent exploitation of system weaknesses that the deviations may create. OCIO had not approved the majority of deviations for noncompliant settings noted in SCAP scan testing. COE and OIG requested and received approvals for some of their deviations, but other OAs did not submit requests to OCIO for approvals.

OAs' Configuration Management Procedures Do Not Comply with NIST and DOT Policy

Six OAs—OIG, FMCSA, OST (COE), Research and Innovative Technology Administration (RITA) (Volpe), Maritime Administration (MARAD) (USMMA) and FAA–have security configuration management procedures that do not conform to NIST and DOT's policies because they have not implemented standard baseline configurations for all of the hardware and software they use. OAs must also perform scanning to verify that their system configurations are correct and that they have applied all security patches. OIG, USMMA and an FAA line of business (LoB) did not have sufficient controls over their software

[14] NIST created SCAP to work with IT communities to develop common configuration standards. As part of the SCAP program, NIST-accredited laboratories test tools and submit their results to NIST. If the results are favorable, NIST validates the tool.

scanning capabilities. Furthermore, USMMA and three FAA LoBs, including CSMC, did not have fully developed patch management processes.

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

DOT does not adequately plan security investments as part of its capital planning. FISMA requires agencies to integrate IT security into their capital planning processes. OMB further requires agencies to plan for and track IT security costs throughout each investment's life cycle. According to OST, the Department has no specific policies and procedures for the estimation, tracking, and reporting of returns on security investments. Specifically, we found the following:[15]

- For fiscal year 2012, OCIO reported that it will focus on the development of policy, process, and use of a tool that support OAs' security controls and in funding decisions. But OCIO provided no plan for this effort.

- Five of 13 OAs (38 percent)—FAA, MARAD, RITA, STB, and OST—did not provide adequate information or documentation that identified their methodologies for security funding estimations and criteria for security project selection.

- Five OAs (38 percent)—FMCSA, Federal Railroad Administration (FRA), MARAD, OIG, and Pipeline and Hazardous Materials Safety Administration (PHMSA)—did not receive the fiscal year 2011 IT security funds they requested. FAA and RITA did not provide documentation that they had received security funding. Furthermore, OCIO requested $30 million for security, but did not receive any. OCIO did not provide a plan for the reprioritization of expenditures as a result of this funding issue.

THE DEPARTMENT'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 security of information systems and ensure that the systems can be recovered should a serious breach occur. We found deficiencies in C&A and contingency plan testing, continuous monitoring, oversight of contractor-operated systems, and controls over remote access and account and identity management.

---

[15] We will provide further detail on these findings in our upcoming report on the Department's enterprise architecture program. We will also provide related recommendations in that report.

C&A and Contingency Plan Testing Are Incomplete

As of October 7, 2011, eight systems were unaccredited, meaning they were not authorized to operate (see Table 3). OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires 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. The 8 unaccredited systems represent a notable improvement over last year when we found 41 systems that were unaccredited. This improvement was brought about by MARAD's successful identification and accreditation of its systems.

Table 3: Summary of Systems with Expired C&A

OA	System Name	Expiration Date	Total Systems
FMCSA	FMCSA Service Centers	6/11/2010	1
OST	Correspondence Control Management System	10/31/2010	1
RITA	RITA- Web	5/31/2010	
	RITA- Mission Support	7/30/2009	
	RITA- TSI Infrastructure	1/02/2010	
	RITA-Transtats	5/16/2011	
	RITA-Everbridge Mass Notification System	7/22/2011	5
STB	Case Management System	11/6/2010	1
Total DOT Systems with Expired C&As			**8**

Source: CSAM

Based on our sample of 64 systems, we estimate that 403 of 445 systems, or 91 percent, had complete C&A documentation.[16] However, 239 or 54 percent, did not have adequate security control testing,[17] while only 179, or 40 percent, had both complete C&A documentation and adequate security control testing.[18] See Table 4 for details of our results.

[16] Our estimate has a margin of error of +/-22 or 5.0 percent at the 90 percent level of confidence.
[17] Our estimate has a margin of error of +/-40 or 9.1 percent at the 90 percent level of confidence.
[18] Our estimate has a margin of error of +/-40 or 9.1 percent at the 90 percent level of confidence.

Table 4: Review of 64 Sample Systems' C&A and Contingency Plans

OA	Systems tested	Systems with deficient or no C&As	Systems with inadequate control testing	Systems without contingency plans
COE	2	0	0	0
FAA	33	2	21	0
Federal Highway Administration (FHWA)	3	0	2	0
FMCSA	3	0	1	1
FRA	2	0	0	0
Federal Transit Administration (FTA)	2	0	0	0
MARAD	4	1	4	1
National Highway Transportation Safety Administration (NHTSA)	2	2	0	1
OIG	2	0	1	0
OST	4	0	0	0
PHMSA	2	0	1	2
RITA	2	1	0	0
Saint Lawrence Seaway Development Corporation (SLSDC)	1	0	0	1
STB	2	0	2	2
Total	64	6	32	8

Source: OIG Analysis

DOT also lacks an effective plan for recovery of its IT systems in the event of a disaster or other disruptions, as required by NIST and OMB. Agencies must also periodically test their contingency plans to ensure they will actually work if needed. Of the sample 64 systems, 36, or 56 percent, had missing or inadequate contingency plans or tests (see Table 4).These included the following:

- Untested contingency plans
- Unsuccessful disaster recovery exercises
- No contingency plan training for personnel
- No contingency plan testing approaches
- Inadequate process for data backup
- 40 percent of critical systems had either no alternative processing site or an alternative processing site that was exposed to same risks as primary site
- Tabletop instead of functional exercises performed for critical systems

Without proper C&A and contingency planning, the Department's systems are not properly assessed for risk and independently tested. Consequently, system

weaknesses may not be identified and sufficiently mitigated. Furthermore, without complete contingency testing, systems may not be recoverable from an unplanned shutdown in time to minimize business disruption.

The Department's Continuous Monitoring of Security Controls Is Ineffective

In June 2011, the Department issued policy on continuous monitoring but has yet to develop guidance or issue an approved Departmentwide strategic plan. NHTSA, FRA and FTA have developed internal guidance; however, most OAs are not complying with existing OMB guidance. For example:

- 7 of 13 (54 percent) OAs did not conduct ongoing assessments of security controls;
- 11 of 13 (85 percent) OAs did not have a continuous monitoring strategy; and
- 10 of 13 (77 percent) OAs did not have any continuous monitoring procedures.

The Department's lack of guidance on continuous monitoring of security controls limits OAs' abilities to monitor their systems' security. It also diminishes their ability to respond quickly to new threats, and affects how well the Department implements security solutions in its highly dynamic environment.

The Department Does Not Identify Its Contractor-Operated Systems in Accordance with OMB Guidance

OMB requires agencies to establish and maintain oversight programs, including inventories, for systems operated by contractors or other entities.[19] However, the Department's methods for identifying contractor-operated systems do not comply with OMB's requirements. As detailed in Table 5, DOT reports a decline in inventory of contractor systems from 33 in fiscal year 2010 to 19 in fiscal year 2011. Of the 64 sample systems, DOT had designated 2 as contractor systems. However, we determined that 26 of the 64 systems, including COE, met OMB's criteria for contractor systems. Consequently, DOT is underreporting contractor systems.

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

Table 5: Fiscal Years 2009 Through 2011Comparison of Contractor Systems

	Fiscal Year		
OA	**2009**	**2010**	**2011**
FAA	10	13	8
FHWA	1	0	0
FMCSA	3	4	2
FRA	6	6	0
FTA	5	0	0
NHSTA	2	2	3
OST	14	4	3
PHMSA	3	3	2
RITA	2	1	1
Total	**46**	**33**	**19**

Source: CSAM

DOT's incorrect classification of systems resulted from OCIO's instructions to classify as contractor systems only those that are both owned and operated by contractors. Contractor systems represent higher risk to the Department because it frequently does not manage security controls in such systems. Without an accurate inventory of these systems, the Department cannot know which systems pose these higher risks.

The Department's Controls over Remote Access Remain Deficient

The Department's remote access controls still do not meet Department and NIST policies and guidance on the control of remote system access. For example:

- COE, Volpe, FMCSA, and FAA have not developed procedures that fully comply with NIST guidance for authorizing, monitoring and controlling remote access.
- COE, STB and Volpe require Government and contractor personnel to have only identifications and passwords for remote access to applications. With the exception of FAA and STB, OAs rely on COE for remote access. However, COE's remote access capability does not require multi-factor authentication. There is no multi-factor authentication implemented within DOT, with the exception of certain FAA LoBs.

- MARAD, FMCSA, STB and RITA did not identify all remote devices.
- FAA, FMCSA, and STB's remote devices and computers are not properly secured and monitored. COE informed us that it needs additional resources to ensure that all remote devices are properly secured and monitored.

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

The Department's Account and Identity Management Are Inadequate

We reviewed the 3 of DOT's 19 general support systems for disabled accounts,[20] and found that the Department's account and identity management controls are deficient in several areas, including issuance of accounts, disabling of accounts, distinguishing of user accounts from non-user accounts, deployment of personal identity verification (PIV) cards, and use of dual accounts for administrators. In May 2009, OCIO issued Departmentwide policies to implement security controls for account management, and user identification and authentication. These policies state that OAs and their LoBs are responsible for implementing the requirements, and that Chief Information Security Officer should validate compliance with the procedures.

Network Accounts Are Not Properly Issued to Users

Three FAA LoB networks had accounts that were not properly issued. For example:

- Two LoBs had instances where unauthorized staff submitted and approved requests to create accounts for new users;
- Two LoBs did not sufficiently separate among different staff the duties for creation, modification and disabling of accounts; and
- One LoB did not always verify the authority of account requestors and approvers to create accounts.

We also found instances in which employees had unauthorized membership in network groups. Network account groups assign the same access rights to all members to simplify administration. Employees with unauthorized membership will acquire the group's access rights. We also found one LoB that could not determine whether certain users had group memberships. These improper account creation and privilege assignment processes increase the risk that users may gain unauthorized or excessive access to network functions.

---

[20] These three general support systems are FAA networks that have approximately 58,000 or 75% of the estimated 77,000 DOT active user accounts.

Network Administrators Do Not Disable Accounts in a Timely Manner

User accounts in Department systems had not been disabled after lengthy periods of inactivity. DOT's policy states that information systems should disable user identifiers after 30 days of inactivity for high-impact systems[21] and 60 days for moderate-impact systems.[22] Table 6 details the 5760 accounts, all of them high and moderate impact, that were not disabled in a timely manner. We also discovered active accounts whose users were deceased or retired.

Table 6: Accounts Not Disabled in a Timely Manner

System Name	Disabling Period		System Category		User Accounts
	>30 days	> 60 days	High	Moderate	
AVS-INF (Internal)	✓		✓		356
AVS-INF (External)	✓		✓		2,110
COE	✓		✓		1,048
CSMC IDPS		✓		✓	5
FAA/ATO LAN		✓		✓	1,173
FAA/ARC[a]		✓		✓	144
FAA/ARP LAN		✓		✓	100
FAA/ASH HQ LAN		✓		✓	62
FAA AST LAN		✓		✓	14
FMCSA Service Centers		✓		✓	36
USMMA LAN		✓		✓	644
OIG Infrastructure		✓		✓	45
STB LAN		✓		✓	23

Source: OIG

Note: We were unable to extract data from Volpe LAN and IRMS due to missing information in the network directory.

[a] Includes ARC LANS, AML LAN, RTF LAN, AWA & Hangar 6, CMEL, MMAC File and Print

The disabling of accounts in an untimely manner may lead to unauthorized access to information and systems by individuals who no longer have authorized access.

[21] "Impact" refers to the impact that the loss of a system's confidentiality, integrity, or availability can be expected to have on organizational operations, assets, or individuals. "High impact" would have a severely adverse effect.

[22] DOT CIOP 1351.15, issued May 2009, outlines the disabling period for user identifiers according to impact level. DOT CIOP 1351.37, issued July 2011, requires user identifiers be disabled after 60 days of inactivity. During our review, we followed the criteria established in DOT CIOP 1351.15, which was in effect at the time.

Network Administrators Do Not Properly Distinguish Account Types

NIST requires agencies to segregate account types—individual, group, system, application, guest/anonymous, or temporary—and to distinguish account types between user and non-users. However, the three FAA networks that we tested did not comply with these requirements because the administrators of these networks did not follow DOT's naming standards when they established the accounts. Without accurate identification of user and non-user accounts, the Department cannot properly control access to its information systems. Table 7 provides examples of incorrect account names among these three networks.

Table 7: Summary of Account Naming Errors

Network	Type of Account	Erroneous Account Name	Correct Account Name or Format
FAA AVS	Service	ricoh	sa-ricoh
	Test	ASI1	T_AS I1
	Service Account for AFS700 RJE Printer	RJE-AFS700	sa_RJE-AFS700
FAA ATO	Service	ame530-backup-svc	SRVC-ame530-backup
	Undetermined	AMA100X2	Undetermined
FAA ARC	Undetermined	Archibus1	Undetermined

Source: OIG

FAA Has Not Completed Deployment of Multifactor Authentication for Local Access to Networks

While FAA LoBs use tokens for multifactor authentication for remote access to networks, they have not implemented multifactor authentication for local access. FAA is implementing PIV cards as its two-factor authentication for local access, and is scheduled to complete the process by January 2012. However, one of the systems we reviewed did not have a PIV implementation plan for logical access, including log-on access. Furthermore, FAA is not scheduled to fully implement the use of PIV cards for physical access to systems, such as access to buildings, until December 2014.

Because multifactor authentication has not been fully implemented, DOT cannot sufficiently identify and authenticate authorized users. Individuals who are not properly authenticated may be able to share user identification and passwords.

Lack of full deployment of PIV cards for physical access increases the risk of authorized access to secured facilities.

Not All Network Administrators Have Dual Accounts

None of the three FAA LoBs we reviewed had implemented dual accounts for all administrators. NIST guidance requires agencies to separate duties through assigned system access authorizations including different accounts for different roles. For example, a system administrator who has an email account on the network he or she administers should have an administrator account and a user account. This individual would use only the user account to access email. Because administrator accounts have greater access to computer resources, the use of such accounts to perform non-administrator functions increases the likelihood that malware such as viruses will infect DOT networks.

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

The Department's remediation of security weaknesses remains ineffective due to weaknesses in oversight and an incomplete POA&M database. FISMA requires a process for the planning, implementation, evaluation, and documentation of actions that address information security weaknesses. OMB policy requires departments to develop POA&Ms for detected system weaknesses and prioritize remediation of the POA&Ms' based on the severity of the weaknesses, which DOT designates as high, medium or low. To facilitate weakness remediation, departments must centrally track all POA&Ms. DOT uses CSAM for this purpose. To evaluate its performance in POA&M management, DOT developed IT Vital Signs, a module that places reports on the Department's intranet and includes a coding system indicating management's remediation success.[23] While IT Vital Signs represents progress, it may not be accurate. For example, DOT's current report indicates that the Department's status across all OAs is average, with all OAs having acceptable, or above average, performance. However, 34 percent, or 1,565 of 4,668 open POA&Ms passed their due dates for resolution, including 374 that are over a year overdue, and 88 that have no target completion dates (see Table 8). The 34 percent overdue represents a 9 percentage point increase over the prior year.

[23] OCIO developed formulas to extract information from CSAM to generate IT Vital Signs' assessment of DOT and OA management's POA&M performance.

Table 8: DOT's Open POA&Ms and Days Overdue

OA and Number of Open POA&Ms		Days Overdue					Summary of Timeliness Issues		
		1 - 60	61 - 90	91 - 120	121 - 365	> 365	No Due Date	Total Overdue	To Become Overdue
COE	15	0	0	3	2	0	0	5	10
OCIO	111	10	0	7	9	46	10	82	29
FAA	3,891	215	17	53	689	263	22	1259	2632
FHWA	108	0	0	0	0	0	0	0	108
FMCSA	1	0	0	0	0	0	1	1	0
FRA	62	35	0	0	0	0	1	36	26
FTA	66	1	0	0	1	1	2	5	61
MARAD	127	5	1	2	0	0	10	18	109
NHTSA	3	0	0	0	0	0	0	0	3
OIG	29	12	3	1	5	8	0	29	0
OST	100	13	1	1	8	1	0	24	76
PHMSA	16	0	0	0	1	0	9	10	6
RITA	29	0	0	0	8	3	18	29	0
SLSDC	4	0	0	0	0	0	0	0	4
STB	106	0	0	0	0	52	15	67	39
Total	**4,668**	**291**	**22**	**67**	**723**	**374**	**88**	**1565**	**3103**

Source: DOT Open POA&Ms in Cyber Security Assessment and Management (CSAM) system as of August 9, 2011

DOT has changed its remediation time requirements twice during the past 2 years (see Table 9). The timeframes in place during our review were flawed because they are shorter for low priority weaknesses than high priority. DOT recognizes this flaw needs to be corrected, but has yet to issue its final revised timeframes.

Table 9: Changes to Time Requirements for Remediation

POA&M Priority	DOT Order 1351.6	DOT Order 1351.30	DOT Order 1351.37 Draft Procedures[a]
High	Remediate within 24 hours	Develop a remediation plan within 90 working days	Remediate within 30 working days
Moderate	Remediate within 20 working days	Remediate within 90 working days	Remediate within 90 working days
Low	Remediate within 60 working days	Remediate within 30 working days	No remediation period specified

Source: OIG
[a]DOT Security Assessment and Authorization Guide, dated July 2010 (DRAFT)

In addition, OAs did not record all known weaknesses in CSAM. For example, we detected over 3000 weaknesses in our 64 sample systems for which we could not locate a POA&M in CSAM or other documentation in the C&As. We also found that 32 systems had incomplete testing of minimum security controls, and consequently, may have unidentified weaknesses.

Without an adequate POA&M remediation process, the Department cannot ensure that its systems are adequately secured and protected. Weaknesses that are unaccounted for, unresolved or unmitigated for extended periods of time create the risk of exploitation that may compromise systems' availability and data integrity.

CONCLUSION

The Department's ability to safeguard its IT systems from hackers and other unauthorized users depends on its ability to implement and maintain adequate security controls as prescribed by OMB and NIST, while keeping its networks available to legitimate users. As technology progresses, so do the risks involved in its use and the need to maintain a state-of-the-art cybersecurity program that can respond quickly and effectively to any threat. Until DOT takes action to follow requirements and address its persistent cybersecurity weaknesses it will continue to expose its IT systems to these 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 closing recommendations we have previously made:

Information Security Policy

1. Address these policy and procedural weaknesses:

    - Issue information security policy for OST.
    - Enhance existing policy to address security awareness training for non-computer users, address security costs as part of capital planning, correct the definition of "government system", and address the identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications.
    - In conjunction with the OA CIOs, execute a strategy to ensure that sufficient procedural guidance exists for DOT and the OAs.

Enterprise-Level Weaknesses

2. 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.

Information System Security

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

AGENCY COMMENTS AND OIG RESPONSE

A draft of this report was provided to the Department’s CIO on October 24, 2011. On November 9, 2011, we received the Department CIO’s response, which can be found in its entirety in the Appendix.

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 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
Martin Gertel, 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 September 14, 2011, the Office of Management and Budget (OMB) issued M-11-33, FY 2011, *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 OMB template.

To meet FISMA and OMB requirements, we selected a representative subset of 64 of 445 departmental systems (see Table 10) and reviewed the compliance of these systems with NIST and OMB 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. In order to gain greater insight into information security at the OA level, we doubled our sample size from the 30 used in the prior year. To evaluate FDCC compliance within the Department, we selected a stratified sample of 903 out of 90,169 devices to be scanned for compliance. We created a script to extract the test results of FDCC controls from 437 out of 903 devices that were available for scanning.

For account and identity management, we reviewed 3 of the largest of DOT's 19 general support systems. These three systems are FAA networks that comprise 75 percent or 58,000 of DOT's active user accounts. 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, 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.

Table 10: OIG's Representative Subset of DOT Systems, by OA

No.	System	Impact Level	Contractor System? [b]
Federal Aviation Administration			
1	Business Communications System	Moderate	No
2	Common Operating Environment	High	Yes

No.	System	Impact Level	Contractor System? [b]
3	ATO Network	Moderate	No
4	Interim Voice Switch Replacement System	Moderate	Yes
5	Investment Management Tool	Moderate	Yes
6	Air Route Traffic Control Center Critical and Essential Power System Power Monitoring System	Low	No
7	Aeronautical Mobile Communications System	Moderate	Yes
8	AVS Registry System	High	No
9	Backfill and Overtime System	Moderate	Yes
10	Simulator Inventory and Evaluation Scheduling System	Moderate	No
11	Capability and Architecture Tool Suite	Low	Yes
12	Runway Safety Tracking System	Low	Yes
13	Automated Desktop Support	Low	No
14	Low-Level Windshear Alert System	Moderate	No
15	Regulatory Guidance Library	High	No
16	Quality Management Information Technology System	Moderate	No
17	Flight Data Input/Output	Low	Yes
18	Host Interface Device / National Airspace System Local Area Network	Moderate	No
19	Multi-System Access Tool - Airman & Aircraft	Moderate	No
20	Weather System Processor	Moderate	No
21	Information Resource Management System	Low	No
22	Enterprise Services Center Business Systems	Moderate	No
23	WJHTC Enterprise Data Center	Moderate	No
24	Performance Data Analysis and Reporting System	Moderate	Yes
25	Corporate Work Plan	Moderate	No
26	Automated Weather Observation System Data Acquisition System	Low	No
27	Terminal Doppler Weather Radar	Moderate	No
28	System Architect	Low	No
29	Project Document Library	Moderate	No
30	Remote Maintenance Monitoring System	Moderate	No
31	Office of Aviation Safety Infrastructure	High	No
32	Risk Based Resource Targeting	Moderate	Yes
33	AVS Electronic Form Service	Moderate	No
34	Cost Accounting System	Moderate	No
35	Advanced Qualification Program	Low	Yes
Federal Highway Administration			
36	Course Management and Training System	Moderate	Yes
37	Motor Fuels and Finance Analysis System	Low	Yes
38	National Bridge Inventory System	Moderate	Yes

Exhibit A. Scope and Methodology

No.	System	Impact Level	Contractor System? [b]
Federal Motor Carrier Safety Administration			
39	Analysis and Information	Moderate	No
40	Licensing and Insurance	Moderate	No
41	National Registry of Certified Medical Examiners Web Site	Low	Yes
Federal Railroad Administration			
42	CAB Technology Integration Laboratory	Low	No
43	Railroad Credit Risk Assessment System	Low	Yes
44	Financial Management System	Moderate	Yes
Federal Transit Administration			
45	FTA Inter/Intranet	Moderate	Yes
Maritime Administration			
46	USMMA LAN	Moderate	Yes
47	USMMA Student Information System	Moderate	Yes
48	Port of Anchorage	NC [c]	Yes
49	Mariner Outreach System	Moderate	Yes
National Highway Transportation Safety Administration			
50	Support Delivery Services Low Impact System	Low	No
51	Mgmt Gov't Resource Low Impact System	Low	Yes
Office of Inspector General			
52	US DOT/OIG Infrastructure	Moderate	No
53	US DOT/OIG TIGR System	Moderate	No
Office of the Secretary of Transportation			
54	Parking and Benefit Transit System	Moderate	Yes
55	Grants Information System	Low	Yes
56	Rulemaking Management System	Moderate	Yes
57	Delphi	Moderate	No
Pipelines and Hazardous Materials Safety Administration			
58	Hazmat Intelligence Portal	Moderate	Yes
59	FEDStar	Low	No
Research and Innovative Technology Administration			
60	RITA Web	Moderate	No
61	External SharePoint	NC [c]	No
SLSDC			
62	Financial Management System	Low	No
STB			
63	Case Management System	Moderate	No
64	Local Area Network	Moderate	No

Source: OIG

[a] See Exhibit B for full Operating Administration names.

Exhibit A. Scope and Methodology

[b] DOT Cyber security Definition of Contractor System
[c] Not Categorized

As required, we submitted to OMB qualitative assessments pertaining to DOT's information security program and practices. OMB requires that our FISMA submission include information from all OAs, including OIG. 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 2011 and October 2011. We conducted our work at departmental and OA Headquarters' offices in the Washington, D.C., area as well as regional offices in Oklahoma City, Melbourne, Florida, and King's Point, New York. 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.

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

- *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 A. Scope and Methodology

EXHIBIT B. DOT OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Table 11: OA System Inventory Counts for Fiscal Years 2011 and 2010

	Fiscal Year	
Operating Administration[a]	**2011**	**2010**
Federal Aviation Administration	297	290
Federal Highway Administration	21	22
Federal Motor Carrier Safety Administration	18	21
Federal Railroad Administration	13	13
Federal Transit Administration	5	5
Maritime Administration	25	21
National Highway Traffic Safety Administration	11	11
Office of Inspector General	2	2
Office of the Secretary	31	33
Pipeline and Hazardous Materials Safety Administration	5	6
Research and Innovative Technology Administration	14	13
Saint Lawrence Seaway Development Corporation	1	1
Surface Transportation Board	2	2
Total Systems	**445**	**440**

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

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

EXHIBIT C. Status of Prior Year's Recommendations

Table 12: OIG Recommendations for Fiscal Year 2010, and Their Status

No.	Status	Recommendation
1	Partially 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	Open	To the extent the OAs require their own guidance, review guidance to verify compliance with department policies and procedures.
3	Open	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	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.

No.	Status	Recommendation
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	Open	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	Open	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	Open	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.
19	Open	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.

Exhibit C. Status of Prior Year's Recommendations

No.	Status	Recommendation
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	Open	Perform periodic reviews of active user accounts and network devices to identify accounts that need to be disabled.
25	Open	Work with OAs to identify and logically segregate user accounts and service (role) accounts.
26	Open	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

Exhibit C. Status of Prior Year's Recommendations

Table 13: 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.
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.

Exhibit C. Status of Prior Year's Recommendations

No.	Status	Recommendation
15	Closed	Monitor, and report to the Deputy Secretary, Operating Administrations' progress in resolving long overdue security weaknesses, reestablishing target completion dates in accordance with departmental policy, providing cost estimation for fixing security weaknesses, prioritizing weaknesses, and recording all identified security weaknesses in plan of actions and milestones.
16	Open	Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.
17	Open	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.
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. Status of Prior Year's Recommendations

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis C. King	Former Program Director
Nathan Custer	Program Director
Michael Marshlick	Project Manager
Lissette Mercado	Project Manager
Gerald Steere	Computer Scientist
James Mallow	Project Manager
Martha Morrobel	Information Technology Specialist
Tracy Colligan	Information Technology Specialist
Felicia Moore	Information Technology Specialist
James Mullen	Information Technology Specialist
Nileshkumar Patel	Information Technology Specialist
Jason Mott	Information Technology Specialist
Jenelle Morris	Information Technology Specialist
LaKarla Lindsay	Referencer
Petra Swartzlander	Statistician
Susan Neill	Writer-Editor

APPENDIX. MANAGEMENT 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: NOV -- 9 2011

From: Nitin Pradhan
DOT Chief Information Officer

Reply To Attn. of:

To: Calvin L. Scovel III
Inspector General

DOT Achieved Considerable Cybersecurity Progress in 2011

During the past year, the Department made significant progress in addressing cybersecurity goals and vulnerabilities by leveraging the limited available resources to implement key Federal and departmental initiatives. These efforts are complicated by the fact that our systems must be operational around the clock every day of the year, and any changes must be completed while "keeping the lights on," to support the critical day-to-day operations of the Department of Transportation (DOT). In addition to the OIG report's recognition of our progress in issuing policies, implementing procedures, and providing cybersecurity awareness training throughout the Department, we also made considerable progress implementing focused efforts on some of the most pervasive threats to critical business support operations, including:

- ***Stabilized and Upgraded E-mail*** -- The DOT CIO prioritized resources to address critical issues with enterprise e-mail. Actions included increasing the storage available for replication of e-mail to an alternate site; upgrading server hardware and software; and implementing Microsoft Exchange 2010 to bolster the security and privacy of e-mail, a key Federal priority to reduce exposure to attacks such as *spearphishing* and permit advanced information flow controls to prevent government information from being transferred to non-government computers.

- ***Created IT Vital Signs*** -- We began implementing the IT Vital Signs performance management dashboard as part of a continuous monitoring strategy to increase visibility into cybersecurity performance and compliance and to assist DOT operating administrations and other stakeholders in improving their security postures.

- ***Established Automated Data Feeds*** -- The DOT CISO and staff worked with the Federal Aviation Administration (FAA), the Cyber Security Management Center

(CSMC) and the CIO's own Information Technology Shared Services (ITSS) team to implement Department of Homeland Security (DHS) initiatives to improve cyber-situational awareness with Automated Data Feeds. Automated data feeds, which provide asset hardware and software information, assessment of vulnerabilities, status of compliance with secure configuration requirements, and the status of patches applied to the asset, were put in place to support the two largest technology infrastructure components in the Department. Since January 2011, the Department has used this important data to further improve cybersecurity. This data is providing vital information to improve processes; enhance visibility across Departmental networks; and develop repeatable processes for core cybersecurity program controls of asset management, vulnerability assessment, configuration management, and patch management.

- ***Expanded Trusted Internet Connections (TIC)*** – In response to recommendations arising from the Federal CyberStat assessment process, the Department fully implemented TIC version one critical capabilities. DOT's internet connections are protected by the DHS Einstein program and are being monitored for suspicious and malicious activity by both DHS and DOT. The Department continues to progress on migrating external connections to its TICs for improved security and is expected to complete this work before the end of fiscal year 2012.

- ***Established Domain Name System Security Extensions (DNSSEC)*** -- DOT implemented DNSSEC on all of the Department's top level .GOV domains. This change resulted in additional internet-related security through data authentication and integrity verification that increases trust in DOT web sites and e-mail communications.

- ***Implemented Personal Identity Verification (PIV) cards*** -- DOT made tremendous progress issuing PIV cards to Federal employees throughout the Department—a time consuming, logistically complex, and costly endeavor that provides enhanced capabilities for both physical and logical access.

- ***Revamped Cybersecurity Leadership*** -- Senior DOT leadership enhanced the DOT cybersecurity program organizational structure to stand shoulder-to-shoulder with other cabinet-level Federal Departments by creating a new executive cybersecurity leadership position that will be responsible for overall cybersecurity management including building and maintaining Department-wide consensus and maintaining progress.

- ***Created Roadmap for Enterprise Authentication Services*** -- The DOT CIO prioritized resources to implement an enterprise authentication service. This service will enable employees to reduce the number of passwords and use DOT-issued PIV cards to access applications. The Department has integrated three large systems via this employee-originated initiative. We produced a roadmap for incorporating other agency systems and enabling the use of the PIV card for employee login over the next two years.

Appendix. Management Comments

- ***Solidified Vision for Secure Mobility Technologies*** -- The DOT CIO implemented a plan to address the telework and mobility needs of the Department, in keeping with the Department's Strategic Plan and goals of reduced congestion, environmental stewardship, and security preparedness. The CIO's plan included the development of security standards, policies, and procedures for ensuring the protection of agency information on mobile devices; an active pilot to test the standards and policies in the DOT environment; and the evaluation of technologies to improve the management and security of mobile technology.

- ***Expanded Enterprise Cybersecurity Related Governance*** -- DOT achieved significant progress in planning and implementing governance structure and activities relating to cybersecurity, including:

    - **IT infrastructure modernization plan and roadmap** -- The DOT common operating environment underwent extensive analysis that addressed DOT-wide infrastructure security, solution architectures, and evolving customer demands (e.g., mobility), to formulate a three-year action plan.

    - **Cybersecurity Integrated Project Team (IPT) and Steering Committee** -- The DOT CIO established a Cybersecurity IPT composed of the DOT CISO and security personnel from Office of the Secretary (OST) and Operating Administrations (OAs) to provide focused effort on enhancing cybersecurity.

    - **Cybersecurity Policy Working Group** -- The DOT CISO established a cybersecurity policy working group consisting of security personnel from the OAs to focus specifically on a comprehensive update to Departmental policy and procedures.

    - **Cloud Management Group** -- The DOT CIO established a Departmental cloud management group to oversee and guide the agency's evaluation of the potential implications of expanding use of secure cloud services.

Achieving Cybersecurity Progress with Focus and Accountability

Maintaining and improving the security of our critical business information systems is an absolute priority for the Department. My staff is in the process of closely reviewing the OIG draft report and will provide a detailed plan of action, and milestones, addressing and prioritizing each of the OIG recommendations before the end of the calendar year. We will establish priorities and recognize modal accountability in formulating plans to move forward.

Establishing Priorities for 2012

Resources are increasingly constrained and it is unlikely that our cybersecurity program will receive the additional resources as anticipated in our earlier planning. As a result, it is neither realistic nor plausible to commit to addressing all of the issues described in the OIG draft report in a single year. While the issues discussed in the OIG draft report are integral to

Appendix. Management Comments

FISMA objectives, it is imperative that we focus our constrained resources on the highest priority actions.

At this point, we anticipate focusing our cybersecurity efforts during 2012 to improve perimeter security, implement automated continuous monitoring, and move toward full implementation of PIV-centric multifactor authentication as resources become available. My office continues to collaborate with the various National Security staff members supporting the Federal Cybersecurity Coordinator, the Office of Management and Budget, and DHS to coordinate and achieve these efforts. To the extent that funding may be less than anticipated, effectively prioritizing these initiatives will ensure that all available resources are focused on the highest priority actions for the Department.

Maintaining Accountability Throughout the Department

While my office establishes and conveys policy through numerous channels to maintain a sense of cohesive direction for the Department's cybersecurity efforts, in most cases, implementation must occur in the Operating Administrations. In order to gain the maximum benefit from limited resources and increase accountability, it would be highly constructive for future OIG efforts to provide detailed information in its reports segmented by Operating Administration. This would facilitate the Department's ability to focus its efforts and increase accountability. Such reporting is consistent with the current financial audit process and would reduce duplicative reporting. Many of the key actions that must be taken to improve cybersecurity will depend on the coordinated and collaborative efforts of the Office of the Secretary (OST) and the Operating Administrations. The DOT OCIO will support progress through defining, developing, and aggressively tracking standards, policies, plans and roadmaps. Further, the Operating Administrations should implement improvements based on established priorities set in a collaborative environment, enumerating specific expectations, and utilizing available data to create tracking metrics to ensure accountability. Further enhancement of IT Vital Signs will help provide meaningful metrics to conduct departmental TechStats to assess progress and establish specific metrics for accountability.

Overall, vigilance and further improvement to our cybersecurity posture is imperative to the effective functioning of the Department, the larger Federal community, and our Nation's transportation systems. We take this responsibility seriously, and we do everything possible to ensure our systems are strong, resilient and managed in accordance with Federal requirements.

Appendix. Management Comments