

**TIMELY ACTIONS NEEDED  
TO IMPROVE DOT'S CYBERSECURITY**

*Department of Transportation*

**Report Number: FI-2011-022  
Date Issued: November 15, 2010**

**Prepared by the  
Office of Inspector General  
U. S. Department of Transportation**



# Memorandum

U.S. Department of  
Transportation

Office of the Secretary  
of Transportation  
Office of Inspector General

---

Subject: ACTION: Timely Actions Needed to Improve  
DOT's Cybersecurity  
Department of Transportation  
Report Number: FI-2011-022

Date: November 15, 2010

From: Calvin L. Scovel III  
Inspector General



Reply to  
Attn. of: JA-20

To: Chief Information Officer

In May 2009, the White House reported the need to secure the Federal Government's digital infrastructure and its information—vital to the economy and national security—from compromise.<sup>1</sup> The Department of Transportation's (DOT) \$3.1 billion annual information technology (IT) portfolio is one of the largest among Federal civilian agencies. DOT's IT budget covers over 400 information systems across 13 Operating Administrations (OA),<sup>2</sup> nearly two-thirds of which belong to the Federal Aviation Administration (FAA). The Department's financial systems manage and disburse approximately \$90 billion in Federal funds annually.

To protect the information systems that support Federal operations and assets from cyber threats, the Federal Information Security Management Act (FISMA) of 2002 requires agencies to develop, document, and implement agency-wide 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).

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;<sup>3</sup> (3) management of information

---

<sup>1</sup> White House Report on Cyberspace Policy Review, May 2009.

<sup>2</sup> For purposes of reporting under the Federal Information Security Management Act of 2002, we consider "Operating Administrations" to include all components listed in Exhibit B.

<sup>3</sup> For purposes of this report, enterprise-level controls are controls that are expected to be implemented department-wide—security training, incident response and reporting, and configuration management—and are not system-specific.

security weaknesses; and (4) system-level security controls. As also required by OMB, we provided various assessments and performance measures to OMB via its Web portal.<sup>4</sup>

We conducted this audit between March 2010 and October 2010 in accordance with generally accepted government auditing standards. Exhibit A details our scope and methodology.

## RESULTS IN BRIEF

During fiscal year 2010, DOT succeeded in providing security awareness training to over 90 percent of its employees, including five OAs that provided this training to 100 percent of their employees. Despite these accomplishments, the Department has not made progress needed to address other critical areas. As a result, DOT's information security program does not meet Federal requirements and is still not as effective as it should be. In addition, the Department has successfully addressed only 2 of the 27 recommendations we made in our last report, issued in November 2009. The following provides details of our findings.

1. The Office of the Chief Information Officer (OCIO) has not developed the required procedural guidance to augment the high-level security policy it issued in 2009 in order for Operating Administrations (OA) to manage information security effectively. Furthermore, some policy lacks important elements. For example, DOT's Chief Information Officer Policy (CIOP) does not address the reporting of contractor operated systems. In September 2010, the OCIO issued a revised plan of action and milestones (POA&M) policy that addressed many of our prior year concerns, but the policy incorrectly prioritizes weakness resolution by providing shorter timeframes for resolving low priority weaknesses than for resolving high ones. These various policy and procedure issues contributed to the other issues we identified.
2. The Department has not made sufficient progress in implementing enterprise-level controls. For example, DOT is still unable to effectively track how many contractors it has on board, has no controls to confirm that all major security incidents reported to the Department of Homeland Security (DHS) were actually received by DHS, and does not have security baseline configurations for all of its systems. Furthermore, the Department's Common Operating Environment<sup>5</sup> (COE) compliance with

---

<sup>4</sup> OMB has designated this information as "For Official Use Only." Consequently, our submission to OMB is not contained in this report.

<sup>5</sup> The COE provides network infrastructure support to DOT Headquarters and remote offices, except FAA and FMCSA field sites.

Federal Desktop Core Configuration (FDCC) requirements,<sup>6</sup> which prescribe secure settings for Windows XP software, actually declined since our last review. Only four OAs reported having tools to verify FDCC compliance. The Department's largest OA, FAA, does not use such tools and is unable to determine whether its networks comply with FDCC requirements. Our tests at FAA headquarters revealed numerous instances of FDCC non-compliance without the required documentation to justify the non-compliance.

3. The Department has not effectively identified, tracked, or prioritized information security weaknesses in its POA&Ms to efficiently resolve these weaknesses. The Department tracked approximately 4,800 weaknesses but did not remediate 1,200 of them (25 percent) within approved timeframes. The Department also did not assign a scheduled completion date to 240 weaknesses and an estimated remediation cost to 404 weaknesses.
4. DOT did not establish adequate controls to protect its systems or to recover them in the event of a disruption. As of the end of fiscal year 2010, the Department had not certified and accredited 41 systems (approximately 10 percent of the total number), including several high-impact systems, for operation. Our review of a statistical sample of 33 out of 436 systems found that approximately half had one or more of the following deficiencies: (1) the certification and accreditation did not meet National Institute of Standards and Technology (NIST) standards; (2) the contingency plan testing was insufficient; and/or (3) the required annual testing did not meet NIST standards. The Department also lacked adequate controls over continuous monitoring, oversight of contractor-operated systems, remote access and account management. For example, the Department does not use two-factor authentication to secure remote access to its systems. We also identified network accounts assigned to deceased individuals.

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

---

<sup>6</sup> The National Institute of Standards and Technology, the Department of Defense, and the Department of Homeland Security developed security configuration settings for certain Windows operating systems, including XP. OMB mandated agencies to adopt these settings, which are referred to as FDCC requirements.

## BACKGROUND

Ensuring a secure global digital information and communications infrastructure is one of the President's seven guiding principles in protecting the American people.<sup>7</sup> As the White House has reported, both the Federal Government and the private sector face new cybersecurity threats, including terrorists and international crime groups that target U.S. citizens, commerce, critical infrastructure, and the Government by attempting to compromise computer-based information. Undeterred, these individuals could undermine national security and degrade civil liberties.

In October 2008, we reported that the Department's information security program and practices were not effective.<sup>8</sup> Specifically, we found that DOT had not established adequate policies, procedures, and training to identify weaknesses in information security and protect computer systems and networks or recover them should an incident occur, including those containing personally identifiable information (PII). We made 27 specific recommendations aimed at addressing these deficiencies. To date, DOT has addressed all but one of those recommendations.

In November 2009, we reported that the Department had issued its information security policy—the first step in building a sustainable information security program—and improved the COE's FDCC compliance.<sup>9</sup> However, the Department had not made sufficient progress in other areas. As a result, the Department's information security program was not as effective as it should be and did not meet all Federal requirements. We made 27 additional recommendations for addressing critical vulnerabilities that would enable DOT to establish a more mature information security program. Exhibit C lists these recommendations and their implementation status.

New challenges emerged in 2010. Several congressional bills addressed concerns over the effectiveness of FISMA and government-wide information security. The Administration's interest in cybersecurity resulted in the appointment of a Cyber Security Czar. OMB addressed criticism from various parties, including the Government Accountability Office, that its FISMA metrics were not effective by establishing new ones. These new metrics require OIG to assess information security in the eight areas required by the previous metrics plus two new areas: remote access, and account and identity management. For 2010, OMB did not request the OIG to report on privacy issues.

---

<sup>7</sup> White House Issues: Homeland Security ([www.whitehouse.gov/issues/homeland-security](http://www.whitehouse.gov/issues/homeland-security)).

<sup>8</sup> *Audit of Information Security Program*, OIG Report FI-2009-003, October 8, 2008. OIG reports and testimonies can be found on our Web site at [www.oig.dot.gov](http://www.oig.dot.gov).

<sup>9</sup> *Audit of DOT's Information Security Program and Practices*, OIG Report FI-2010-023, November 18, 2009.

## DOT'S INFORMATION SECURITY POLICY AND PROCEDURES REMAIN 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 information security policies that direct the security efforts by DOT's OAs.<sup>10</sup> However, some of these policies remain in the review process, while the Department has not initiated action on others. Meanwhile, the OAs have either limited or no procedural guidance provided to instruct them on how to effectively and consistently implement information security. In Table 1, we note areas that the Department should consider in its development of adequate guidance to OAs.

***Table 1: Deficiencies in Policy and Procedures***

<b>FISMA Security Program Area</b>	<b>OIG's Evaluation</b>
<b>Certification and Accreditation (C&amp;A) of Controls</b>	
The assessment of security controls to determine if the controls have been implemented effectively.	C&A procedures do not sufficiently guide agency personnel in effectively managing the security for the life of the system.
<b>Continuous Monitoring of Controls</b>	
Required as part of the security authorization process for ensuring that controls remain effective over time.	Continuous monitoring policy is inappropriately high- level and does not sufficiently guide agency personnel in identifying and documenting the security controls inherited from other systems.
<b>Plans of Action and Milestones (POA&amp;M)</b>	
Tracks the measures implemented to correct security weaknesses to eliminate vulnerabilities.	The revised policy emphasizes correcting low weaknesses in short timeframes while allowing considerably more time to correct high and moderate weaknesses. No guidance exists for categorizing weaknesses or on the use of the central database for documenting and tracking POA&Ms.

<sup>10</sup> DOT's 13 OAs are referred to in this report by their acronyms. For a list of the OAs and their' acronyms, see Exhibit B.

<b>FISMA Security Program Area</b>	<b>OIG's Evaluation</b>
<b>Security Awareness and Specialized Training</b>	
Annual training required by FISMA for government and contractor personnel.	The policy and procedures are not sufficiently developed to guide OAs in identifying, tracking and validating contractors requiring annual security training.
<b>Account and Identity Management</b>	
Controls for managing and monitoring network accounts.	The departmental procedures are not sufficiently developed to guide OAs in establishing controls. For example, guidance does not address account naming standards. In addition, operating procedures for personal identity verification (PIV) cards are not complete. For example, these procedures do not address termination of PIV cards.
<b>Configuration Management</b>	
Policy and procedures that ensure that all system owners have implemented approved security control baselines.	Does not include detailed guidance for managing policy requirements. For example, little guidance exists on the development of inventories of technology products and adoption of secure baselines. There are also no procedures for documenting and approving FDCC deviations.
<b>Contractor Oversight</b>	
Monitoring of the effectiveness of support system security provided or managed by contractors, or other agencies or sources.	Neither policy nor procedures contain detailed guidance for reporting to OMB on contractor-operated systems. The policy also does not provide standard contract language regarding contractor compliance with Federal security requirements.
<b>Remote Access</b>	
Components for telework and remote access, including client devices, servers, and internal resources, should be secured against known weaknesses, including the lack of physical security controls, use of unsecured networks, connections between infected devices and internal networks, and the availability of internal resources to external hosts.	Policy and procedures on remote access do not establish an effective approach to identifying, monitoring, tracking and validating users and equipment that remotely access DOT networks and applications.

Source: OIG Analysis

The lack of adequate department-wide guidance on addressing security requirements increases the likelihood that OAs will create internal practices and ad-hoc procedures which may not comply with OMB or DOT requirements. Furthermore, the deficiencies in DOT's information security policies and procedures have contributed to the other weaknesses documented in this report.

## **DOT'S ENTERPRISE-LEVEL CONTROLS—SECURITY TRAINING, INCIDENT REPORTING, AND CONFIGURATION MANAGEMENT—ARE INADEQUATE**

DOT's department-wide controls—those that must be implemented at the enterprise level—are still inadequate. Because it cannot track the number of contractors it has employed, DOT does not know how many of its contractors have received the required security training. Though a significant number of employees received specialized training, certain key employees did not. The Department has not provided evidence that all security incidents, including those that may have breached sensitive information, were reported to the Department of Homeland Security. Furthermore, DOT did not demonstrate sufficient progress in its management of configuration baselines, including the FDCC baselines for Windows XP and Internet Explorer.

### **DOT Cannot Accurately Track Contractors' Security Awareness Training**

FISMA calls for the building and maintenance of comprehensive security awareness training programs which ensure that, before receiving access to agency information systems, all users<sup>11</sup> are adequately trained in their security responsibilities and how to fulfill those responsibilities. DOT policy requires that Line of Business and OA CIOs ensure that all DOT information system users receive basic security awareness training before being authorized to access the system, and at least annual training thereafter, as well as updates on system changes.

However, the Department has no system that effectively tracks all contractors working for the Department. For example, the Department's Investigative Tracking System<sup>12</sup> (ITS) lists over 54,000 contractors in active status—41,000 more than the Department reported to us as having access to its networks. The Department's Office of the Chief Information Officer (OCIO) and the Director of

---

<sup>11</sup> Users may include employees, contractors, foreign or domestic guest researchers, other agency personnel, visitors, guests, and other collaborators or associates requiring access.

<sup>12</sup> The Investigative Tracking System is intended to house the social security numbers of current DOT employees and active contractors and other personally identifiable information, including information on passports, visas and home addresses.



Security stated that ITS was not created to track active contractors, but rather to store information related to pre-hiring background investigations of both employees and contractors; this information is intended to remain stored as long as the personnel remain employed with the Department. However, the officials acknowledged that the Department has no authoritative system to track active contractors and that ITS is the one system that could do this. The Office of Security also informed us that they have requested that OAs assist them in reconciling the numbers in ITS with the actual number of contractors working for the Department. Until this reconciliation occurs, the Department will not have an efficient and effective method of providing security awareness training to contractors and tracking those contractors that have completed it.

Because OAs do not have capabilities for tracking all employed contractors, they have no assurance that all contractors have received security awareness training. Some OAs have developed their own methods for determining percentages of contractors that have completed training, but these methods are labor-intensive and rely on information from systems that do not contain reliable data. For example, one mode stated that, based upon instruction from the Department, it attempted to match contractor names in ITS, despite its known unreliability, with those in COE's active directory and with self-assessments of numbers of its employed contractors. As discussed below, however, COE's active directory also has reliability issues. Because of the reliability problems in both ITS and the COE active directory, using the two systems to identify active contractors is unlikely to produce reliable data.

While ninety-five percent of approximately 58,000 DOT employees received security awareness training in fiscal year 2010, over 3,000 employees did not. Contractor tracking issues along with the incomplete training of employees in security awareness represent significant security risks to the Department. Personnel without security awareness training are more likely to become victims of social engineering or commit acts that compromise information security.

### **Not All Department Employees with Significant Security Responsibilities Receive Required Specialized Training**

DOT policy requires OAs to determine the content of specialized security training based on the specific requirements of their organization and the systems that employees and contractors have access to. Specifically, DOT policies require OAs to provide personnel that have access to system-level software—system owners and system and network administrators—with specialized security training adequate for performing their duties.

The Department reported 851 employees with significant security responsibilities. Although DOT reported that these 851 employees received specialized security

training, our analysis, as shown in Table 2, indicates that approximately 61 personnel in key security related job categories did not receive the training,<sup>13</sup> including six OA Chief Information Officers, two modal Information Security Officers, and ten modal Authorizing Officials.

**Table 2: Job Functions and Employees Requiring Specialized Security Training<sup>a</sup>**

Categories	FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OIG	OST <sup>b</sup>	PHMSA	RITA	SLSDC	STB	Reported	Not Reported
Chief Information Officer	7	1	0	0	1	0	1	1	2	0	0	0	1	14	6
IT Security Officer	56	2	1	5	3	0	1	1	1	0	4	1	1	76	2
System Administrator	2	84	0	0	1	0	37	12	0	1	0	0	0	137	7
System Designer/ Developer	100	82	0	0	7	0	0	3	0	17	0	0	0	209	8
Network Administrator	4	0	0	0	0	0	1	0	2	1	0	0	0	8	9
Database Administrator	4	3	0	0	3	0	1	1	0	3	0	0	0	15	7
Certification Reviewer	0	14	0	0	0	0	1	0	0	0	0	0	0	15	11
Authorizing Official (AO)	0	1	0	0	0	0	1	0	0	0	0	0	0	2	11
Other	169	36	9	5	58	18	36	0	10	29	4	1	0	375	N/A
<b>Total</b>	<b>342</b>	<b>223</b>	<b>10</b>	<b>10</b>	<b>73</b>	<b>18</b>	<b>79</b>	<b>18</b>	<b>15</b>	<b>51</b>	<b>8</b>	<b>2</b>	<b>2</b>	<b>851</b>	<b>61</b>

Source: OIG Analysis

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> OST identified 15 personnel that received specialized security training and were included in the total, but we found that 12 of these 15 reported that the NSA security briefing was considered specialized training. It is our opinion, however, that this briefing does not comply with NIST.

As we noted in last year's review, DOT policy does not identify specific job functions, such as the CIO, Information Security Officer, and Database

<sup>13</sup> Our scope was limited to 8 job categories.

Administrator, that require specialized security training. As a result, the Department is at risk of not appropriately securing its information systems. Furthermore, without specialized security training, Department employees may not develop the skill sets needed to perform their security responsibilities.

### **The Department's Reporting Process Does Not Ensure that All Security Incidents Are Actually Reported to the Department of Homeland Security**

OMB policy requires that each security incident be reported to the Department of Homeland Security's U. S. Computer Emergency Readiness Team (US-CERT). According to DOT, when an incident occurs, the OA reports it to DOT's Cyber Security Management Center (CSMC), which analyzes the report, categorizes the incident by type, and reports each incident to US-CERT. Subsequently, US-CERT generates a reference number for certain reported incidents. However, we found that, of 2,859 incidents reported to US-CERT by DOT between July 1, 2009 and August 15, 2010, 129 (4.5 percent) did not have a US-CERT reference number (see Table 3) or other evidence to ensure receipt. We also found that 248 (8.7 percent) did not have corresponding US-CERT Report Dates.

**Table 3: Summary of Incidents Missing US-CERT Reference Numbers**

<b>US-CERT Category<sup>a</sup></b>	<b>Incidents Missing Reference Numbers</b>	<b>Percentage</b>
Category 1: Unauthorized Access (e.g., PII breach)	18	14
Category 2: Denial of Service (DOS)	0	0
Category 3: Malicious Code	99	77
Category 4: Improper Usage	11	9
Category 5: Scans/Probes/Attempted Access	1	1
<b>Total Security Incidents</b>	<b>129</b>	<b>100<sup>b</sup></b>

Source: OIG Analysis

<sup>a</sup>US-CERT Category 0 (Exercise/Test) and Category 6 (Unconfirmed Incidents) were not in our analysis because they are not required to be reported to US-CERT.

<sup>b</sup> Totals may not add due to rounding

Without a US-CERT reference number or an approved process to verify DHS received the incidents, DOT cannot determine whether or not the DHS received

the reports, undermining the Government's ability to properly coordinate among Federal agencies in order to defend against cyber attacks.

### **The Department Has Not Fully Met Configuration Standards**

FISMA 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. Earlier in the year, we found that the Department's American Recovery and Reinvestment Act (ARRA) websites had significant vulnerabilities resulting from incorrect configurations.<sup>14</sup> More recently, we found configuration deficiencies in FDCC compliance, and the absence of a full implementation of configuration baselines throughout the Department. Without complete implementation of configuration standards, the Department has little assurance that it is sufficiently protecting its information systems from known, exploitable software weaknesses. Inadequately configured software also increases security vulnerabilities that could impact DOT's mission and business operations.

#### *Operating Administrations Are Not in Compliance with Federal Desktop Core Configuration Requirements*

OMB requires agencies that have deployed certain software, such as the Windows XP operating system, to adopt NIST security configurations settings known as the FDCC requirements. OMB also requires that departments meet all NIST configuration settings in order for them to be 100 percent compliant. We statistically sampled 63 employees that use Government-provided computers from 7,756 personnel in the Washington area. Based on this sample, we estimate that the number of employees with FDCC compliant computers is somewhere between 0 and 283 out of the 7,756.<sup>15</sup> In addition, all 14 individuals from one FMCSA field site were selected based on geographical location and their Government-provided computers were representative of FMCSA field sites throughout the US. These remote computers were only 82 percent compliant for Windows XP and 70 percent for Internet Explorer. In aggregate, all the computers tested were 90 percent compliant for Windows XP, and 72 percent for Internet Explorer. None of the computers tested were fully compliant with NIST settings. Table 4 shows the controls tested, passed, and failed.

---

<sup>14</sup> *ARRA Websites Vulnerable to Hackers and Carry Security Risks*, OIG Report FI-2011-006, October 22, 2010. [www.oig.dot.gov](http://www.oig.dot.gov)

<sup>15</sup> The estimate has a 90% confidence with a margin of error of 3.7%.

**Table 4: FDCC Sample Test Results**

	<b>Number Systems Sampled</b>	<b>Total Controls Tested<sup>c</sup></b>	<b>Total Controls Passed</b>	<b>Total Controls Failed</b>
FAA <sup>a</sup>	25			
Windows		9,525	8,414	1,111
Internet		2,875	1,461	1,415
FMCSA Field Site	14			
Windows		5,246	4,323	923
Internet		1,441	1,005	436
ITS (COE) <sup>b</sup>	34			
Windows		12,954	12,411	543
Internet		3,468	3,169	299
OIG	2			
Windows		762	695	67
Internet		204	200	4
STB	2			
Windows		762	435	328
Internet		230	120	110
Department Totals:	77			
Windows		29,249	26,278	2,972
Internet		8,218	5,955	2,264

Source: OIG

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> The Department consolidated Operating Administrations' network infrastructures (e-mail, desktop computing, and local area networks) into a common IT infrastructure.

<sup>c</sup> Totals may not add due to rounding.

One of the Department's controls for ensuring the use of approved configuration settings is creating a uniform image of desired FDCC control settings and applying it to all workstations. However, we found numerous different FDCC settings among workstations that were supposed to be identical. For example, FMCSA

had up to 12 different settings among its computers. While we did not determine the cause for this variance, such differences can be caused by malware or viruses.

OMB requires agencies to use Security Content Automation Protocol<sup>16</sup> (SCAP)-validated tools to certify that their systems comply with FDCC standards. Agencies are also required to manage and monitor the configuration of these standards once deployed to personnel to ensure they are not modified. Only four OAs reported 100 percent coverage of their systems using SCAP-compliant tools. The remaining nine OAs, however, either had less than 100 percent coverage of their systems or did not provide evidence of coverage. For example, FAA did not use a SCAP tool to ensure FDCC compliance for its networks. Without valid testing using approved tools, the degree of FDCC compliance may deteriorate and expose the Department to unexpected vulnerabilities.

Deviations from preferred control settings do occur when an agency determines that the settings impact operations, such as the running of legacy applications. The implementation of such deviations requires high-level review and approval to prevent exploitation of possible weaknesses created by the deviations. However, DOT does not have an adequate process for approving deviations<sup>17</sup> from FDCC requirements. While the Department policy requires OAs to receive approval from the Department's CIO for use of deviations, there is no guidance on how to request a deviation. The majority of deviations noted in our testing had not been approved. While FRA and SLSDC requested and received approvals for some FDCC deviations, COE, FMCSA field sites, and PHMSA submitted deviations but did not receive approvals. Other OAs, including FAA, had not submitted requests for approvals. Without an adequate deviation approval process, the Department cannot assess the necessity of such deviations or attempt to resolve them.

*Operating Administrations' Configuration Management Procedures Do Not Comply with NIST and DOT Policy*

Nine OAs—FAA, FMCSA, FTA, MARAD, OIG, OST, PHMSA, RITA, and SLSDC—have security configuration management procedures that do not align with NIST and departmental policy. For example, PHMSA, FHWA, and FRA have implemented standard baseline configurations, but not for all of the hardware and software they use. Three of these OAs—FAA, OIG and RITA—have no baseline configuration procedures to ensure the security of their systems. Furthermore, none of these OAs' procedures has been reviewed in detail by OCIO due to a lack of available personnel, and OCIO's focus on developing DOT's Cyber Security Strategic Plan.

---

<sup>16</sup> NIST has created the SCAP program to work with the information technology communities to develop common configuration standards. As part of this program, NIST-accredited laboratories test tools and submit results to NIST. If the results are favorable, NIST validates the tool.

<sup>17</sup> A deviation occurs when the parameter for a particular setting is different from the approved parameter. OMB requires that such deviations be approved by the department or agency's accrediting authority.

OAs also should perform scanning to verify that system configurations are correct and that security patches have been applied. Three OAs—FRA, STB, and SLSDC—did not provide documentation of controls over their software scanning capabilities. Five OAs—FHWA, FMCSA, FRA, FTA and RITA—did not provide scanning evidence or confirmation for timely resolution of vulnerabilities. For example, FAA's use of an unsupported Oracle database resulted in untimely patching of the Department's financial system (Delphi) and rendered vulnerability scanning ineffective for that system. In another example, SLSDC has no patch management policy or procedure in place. Moreover, DOT has no department-wide process for managing OA compliance with policy requirements pertaining to inventories of technology products and corresponding security baselines.

## **THE DEPARTMENT CONTINUES TO LACK AN EFFECTIVE PROCESS FOR REMEDIATING INFORMATION SECURITY WEAKNESSES**

FISMA requires a process for planning, implementing, evaluating, and documenting remedial actions to address information security weaknesses. DOT's process is ineffective due to its weaknesses in management oversight and its incomplete POA&M database.

Last year, OCIO began meeting monthly with Operating Administrations to address information security concerns. In fiscal year 2010, however, these meetings were delayed until July 2010 because of changes in OCIO priorities. As evidence of its oversight of OAs' remediation of security weaknesses, OCIO could only point to its review of FHWA's POA&M status. This insufficient oversight of OAs, in turn, contributes to the inadequate resolution of security weaknesses, including the slow implementation of our prior year recommendations. As shown in Table 5, there are:

- 4,794 open POA&Ms or weaknesses;
- 1200 weaknesses, or 25 percent, that are overdue, including 126 that are over 1 year overdue;
- 240 weaknesses that have no scheduled completion dates;
- 404 POA&Ms that did not identify the cost to remediate the weakness;
- 3,594 weaknesses, or 75 percent, that had completion dates that exceeded policy time frames for remediating weaknesses in place at the time; some of these had completion dates scheduled for 4 years in the future.

**Table 5: Summary of Overdue POA&Ms**

Operating Administration <sup>a</sup>	Total Open POA&Ms	1 - 60 days	61 - 90 days	91 - 120 days	121 days - 1 year	> 1 yr	No Target Completion Date	Total Overdue	Future Scheduled Completion Date
DOT Program	106	3	1	8	3	68	5	88	18
FAA	4170	267	78	62	365	0	85	857	3313
FHWA	159	0	0	0	1	0	0	1	158
FMCSA	2	0	0	1	0	1	0	2	0
FRA	11	0	0	3	6	0	2	11	0
FTA	20	0	0	0	1	0	0	1	19
MARAD <sup>b</sup>	111	0	0	0	0	0	111	111	0
NHTSA	1	0	0	0	1	0	0	1	0
OIG	17	8	1	0	4	2	0	15	2
OST	71	6	0	2	6	2	0	16	55
PHMSA	22	1	1	0	0	0	0	2	20
RITA	32	4	0	0	0	1	18	23	9
SLSDC	5	1	0	0	0	0	4	5	0
STB	67	0	0	0	0	52	15	67	0
Total	4794	290	81	76	387	126	240	1200	3594
Percentage		6%	2%	2%	8%	3%	5%	25%	75%

Source: DOT Open POA&Ms in Cyber Security Assessment and Management (CSAM) system as of August 18, 2010

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> 111 POA&Ms reported by MARAD were not assigned a scheduled completion date.

Based on the policy in effect at the time of our review, all 4,794 open POA&Ms were, or were expected to become, overdue. The policy required high-priority weakness to be resolved within 24 hours, moderate-priority ones within 20 working days, and low-priority ones in approximately 3 months. In September 2010, OCIO issued new POA&M policy that significantly changed the timeframes for resolution of weaknesses. However, because of its shorter timeframe for resolving low-priority weaknesses, the policy will likely result in the resolution of low priority weaknesses before high ones. Table 6 summarizes the changes in timeframes.



**Table 6: Changes to Remediation Time Requirements**

<b>POA&amp;M Categorization</b>	<b>Prior Policy-- DOT Order 1351.6, Section 4.5 POA&amp;Ms</b>	<b>Current Policy-- DOT Order 1351.30</b>
High	Remediate within 24 hours	Develop a remediation plan within 90 working days
Moderate	Remediate within 20 working days	Remediate within 90 working days
Low	Remediate within 60 working days	Remediate within 30 working days

Source: OIG

Furthermore, Operating Administrations did not record all identified security weaknesses in the Department's POA&M database for 20 of the 33 systems that we selected for this year's review. In particular, MARAD did not input any known security weaknesses in the POA&M database, including the deficiencies in its systems' certification and accreditation reported last year.

Without a compliant POA&M process, the Department cannot ensure that its systems are adequately secured and protected. Weaknesses that remain unaccounted, unresolved or unmitigated for extended periods of time allow for unnecessary vulnerabilities and exposures that may be exploited, or may otherwise compromise the availability or integrity of systems and data. Furthermore, establishing tighter time frames to address only low priority weaknesses could result in high priority weaknesses requiring more time than necessary to resolve.

## **THE DEPARTMENT'S SYSTEM-LEVEL CONTROLS ARE NOT ADEQUATE TO PROTECT THE SYSTEMS OR ENSURE RECOVERY**

System-level controls protect the security of information systems and ensure that they can be recovered should a serious security breach occur. However, the Department does not effectively manage these controls. Specifically, we found the Department does not know how many systems MARAD owns; certification and accreditation as well as contingency plan testing are incomplete; continuous monitoring is ineffective; oversight of contractor-operated systems is inadequate; controls over remote access are deficient; and controls over account and identity management are also deficient.

## **The Department Does Not Know How Many Systems MARAD Owns**

FISMA requires agencies to develop, maintain, and annually update inventories of the major information systems, including interfaces to external systems that they operate or control. Agencies can then use the inventories to track their systems for annual testing and evaluation, and contingency planning. Developing a complete and accurate inventory of major information systems is an agency's first step in managing its information technology resources, including security.

For FY 2009, we reported that MARAD did not use an appropriate methodology in developing its system inventory. For FY 2010, MARAD has been unable to provide an accurate inventory of its systems. In April 2010, MARAD informed us that it had 18 systems. More recently, the Agency informed us that its system total was anywhere between 23 and 83. MARAD is conducting a review of the number of systems it has and the number of certifications and accreditations it needs to perform. Without a well developed inventory, it is almost impossible to determine whether or not system-level controls are implemented or effective, or to track system security metrics. Furthermore, as system changes occur, it is difficult to reassess system-level controls and to enforce system-level security.

## **Certification and Accreditation and Contingency Plan Testing Are Incomplete**

OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires that systems be reauthorized (i.e., accredited) at least once every 3 years. As of September 30, 2010, at least 41, or 10 percent, of the Department's systems are unaccredited, meaning they were not authorized to operate. Table 7 lists the OA, system name, and date of certification and accreditation expiration for all unaccredited systems, except MARAD, which has at least 23 unaccredited systems, all of which continue to operate.

**Table 7: Summary of DOT Systems with Expired Certification and Accreditation**

OA <sup>a</sup>	System Name	Expiration Date	Total Systems
FMCSA	CoTs DOT ECOM LAN	2/07/2010	
	CoTs DOT LAN	2/07/2010	
	Performance and Registration Info. Sys. Mgmt.	4/26/2010	
	Electronic Information System (EMIS)	6/11/2010	
	Electronic Document Mgmt Sys (EDMS)	6/15/2010	
	Query Central (QS)	6/15/2010	
	Commercial Vehicle Info. Sys and Networks	6/22/2010	
	Compass	8/27/2010	8
FRA	Controlled Correspondence Manager (CCM)	9/06/2010	
	Web Information Services (WIS)	9/06/2010	
	Automated Track Inspection Program (ATIP)	9/21/2010	
	GradeDec.Net	9/21/2010	
	Railroad Safety Advisory Committee (RSAC)	9/22/2010	5
OIG	US DOT/OIG Infrastructure	8/28/2010	
	US DOT/OIG TIGR System	9/18/2010	2
RITA	RITA- Web	5/31/2010	
	RITA- Mission Support	7/30/2010	
	RITA- TSI Infrastructure	1/02/2010	3
MARAD	Multiple Systems	N/A	23 <sup>b</sup>
<b>Total DOT Systems with Expired C&amp;As</b>			<b>41</b>

Source: DOT Expired C&As in Cyber Security Assessment and Management (CSAM) system as of September 30, 2010

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> Estimate

We statistically selected 30 out of 436 systems reported to us. We reviewed 33 systems because one system was made up of 4 subsystems. The results of the 33 are summarized in Table 8. Based on this sample, we estimate that 170 (39 percent) would not fully meet the C&A requirements cited in NIST 800-37, 109 (25 percent) would be deficient in annual testing,<sup>18</sup> and 196 (45 percent) would not be compliant at contingency planning and testing.<sup>19</sup>

<sup>18</sup> Subsequent to the initial authorization of the entire information system, OMB requires agencies to test subsets of their security controls annually, as part of continuous monitoring.

<sup>19</sup> This estimate has a 90-percent confidence level with a margin of error for DOT C&A of +/-19.5, for security control testing of +/-16.8, and for contingency planning and testing of +/-20.2.

**Table 8: Results of Review of Sample of 33 Systems<sup>a</sup>**

	FAA	FHWA	MARAD	NHTSA	OST	RITA	Total	Percentage
Number of Systems Sampled	15	4	7	4	2	1	33	
Systems without C&As or with deficient C&As	8	0	7	0	0	1	16	48%
Systems without sufficient annual testing	5	0	7	0	0	1	13	39%
Systems without comprehensive contingency plans and testing	10	0	7	0	0	1	18	55%

Source: OIG Analysis

<sup>a</sup> See Exhibit B for full Operating Administration names.

Without proper certification and accreditation, the Department lacks a crucial management control that ensures that systems are properly assessed for risk, have been independently tested, and that system weaknesses have been identified and sufficiently mitigated. Without this control, management cannot ensure that systems are operating without unacceptable risks or weaknesses. Furthermore, without complete security and contingency testing, systems may operate with new or unresolved weaknesses and may not be recoverable in time to minimize business disruption.

### **The Department's Continuous Monitoring Is Ineffective**

As noted in our prior report, the Department's policy and procedures on continuous monitoring were not sufficiently detailed to guide agency personnel to conduct effective continuous monitoring of security controls. For FY 2010, OCIO noted that the planned revisions to these departmental procedures will not be implemented until November 2012. Furthermore, the Department does not have an approved strategic plan for continuous monitoring. Without these department-wide procedures, OAs have acted on their own. FAA, FHWA, FMCSA, FRA, and NHTSA developed internal guidance. Overall, however, the OAs are not acting in compliance with existing OMB guidance. For example:

- 12 out of 13 OAs did not effectively review, monitor and validate security controls;
- 9 OAs do not incorporate continuous monitoring results into security status reports or use them to update C&A documents (Security Plan, Security Assessment report, POA&M);
- 9 OAs do not provide authorizing officials and others reports on continuous monitoring.

The lack of procedures for comprehensive continuous monitoring limits OAs' abilities to adequately monitor, in a timely manner, the security of their information systems. It also diminishes their abilities to respond quickly to new threats, and may affect how well the Department can implement security solutions in its highly dynamic environment.

### **The Department's Oversight of Contractor-Operated Systems Is Inadequate**

For 2010, OMB required OIGs to determine whether agencies had established and were maintaining oversight programs for systems operated by contractors or other entities, including inventories of such systems. The Department's methods of identifying contractor-operated systems and related interfaces do not comply with OMB's requirements. Furthermore, some of its information technology contracts do not include language requiring conformance to FISMA.

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

The Department's inventory of contractor systems decreased from 46 to 33 between fiscal years 2009 and 2010, as shown in Table 9. This decrease occurred due to OCIO's instruction to the OAs to count as contractor systems only those that are both owned and operated by contractors. This new definition is not consistent with OMB's guidance, which defines a contractor system as any system operated on an agency's behalf by a contractor or other entity. Furthermore, according to OCIO, no established process exists for reviewing and ensuring the accuracy of OAs' reporting on contractor systems. As a result, OCIO was not aware of inconsistencies in the reporting. Contractor-operated systems represent additional risks to the Department because it frequently does not manage security controls in such systems. Without an accurate inventory of these systems, the Department cannot effectively manage the risks.

**Table 9: FY 2009 and 2010 Comparison of Contractor Systems<sup>a</sup>**

	FY 2009	FY 2010	Difference
FAA	10	13	3
FHWA	1	0	(1) <sup>b</sup>
FMCSA	3	4	1
FRA	6	6	0
FTA	5	0	(5) <sup>c</sup>
NHSTA	2	2	0
OST	14	4	(10) <sup>b,c</sup>
PHMSA	3	3	0
RITA	2	1	(1) <sup>b</sup>
<b>Total:</b>	<b>46</b>	<b>33</b>	<b>(13)</b>

Source: OIG

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> Retired

<sup>c</sup> Re-defined from contractor operated

### *Some IT Contracts Do Not Contain Clauses Regarding FISMA Compliance Requirements*

FISMA and OMB require agencies to ensure that contractors comply with Federal information security requirements. However, OCIO's policy and guidance do not address the inclusion of specific clauses in contracts to ensure that the Department incorporates Federal security requirements into its information technology procurements. For example, we found contracts that did not incorporate Federal computer security language. Furthermore, even though FAA has a standard clause for FISMA compliance, we found that six out of eight FAA contracts did not incorporate this clause. Finally, 12 OAs did not provide evidence that they develop and manage their contractor interface agreements in compliance with OMB policy.

Without the required contract language, up-to-date interface agreements, and oversight, DOT cannot enforce compliance with important information security requirements, or ensure that security risks are reduced in a cost-effective and consistent manner.

### **The Department's Controls Over Remote Access Are Deficient**

NIST provides guidance for agencies on controlling remote access to their systems. In 2007, OMB announced the Trusted Internet Connection (TIC) initiative to reduce and consolidate the number of external access points, including

Internet connections, and ensure that all external connections are routed through an OMB-approved TIC.

We found that the Department's remote access controls are deficient. For example:

- Home computers can be used for internet access to DOT's systems. However, DOT's policy does not provide clear guidance on the safe use of home computers for this access, and only requires users from home to have IDs and passwords for identity authentication in order to gain access. With the exception of FAA, which requires identification tokens in some instances, there is no multi-factor identity authentication in use at DOT.
- Home computers used to access DOT applications are checked for up-to-date operating system patches and virus protection, but they are not checked for FDCC compliance.
- DOT does not conduct real-time monitoring and authentication of equipment that remotely accesses its networks to ensure that only authorized devices are able to connect.
- FAA has an informal agreement that all employees who have faa.gov email accounts will be provided remote access to their email accounts. FAA is in the process of developing a plan to revise its remote access policy and provide it to its CIO for guidance.
- DOT policy lacks specific requirements on use of wireless access to DOT networks; OCIO reported that this policy is currently in revision but provided no completion date.
- CIO does not plan to complete routing all agency external connections through approved Trusted Internet Connection access points until after 2011.

Without effective controls over remote access, DOT cannot ensure that only authorized computers and personnel are accessing its information systems. As a result, there is an increased risk that unauthorized users will deploy malware on DOT's networks or extract sensitive information.

### **The Department's Controls Over Account and Identity Management Are Deficient**

NIST provides guidance for network accounts and identity management. In May 2009, DOT OCIO issued Department-wide policies to implement security controls for account management, and user identification and authentication. These policies state that Lines of Business/OAs are responsible for implementing the policies' requirements, and that the Chief Information Security Officer should validate compliance with the procedures. We reviewed four networks that service about 54,000 users and found that the Department's account and identity

management controls are deficient in several areas, including disabling of accounts, distinguishing between user and non-user accounts, using multi-factor authentication, and using dual accounts for administrators.

*Network Administrators Do Not Disable Accounts in a Timely Manner*

DOT OCIO policy states that information systems should disable user identifiers after 30 days of inactivity for high-impact systems<sup>20</sup> and 60 days for moderate-impact systems. It further states that all system accounts should be configured to automatically lock out inactive users within a specific period of time not to exceed 90 days. Of the approximately 54,000 accounts we reviewed, we found that about five percent had not been disabled after the required period of inactivity. See Table 10 for a description of these accounts. We also found two active accounts whose users were deceased.

**Table 10: Accounts That Were Not Disabled in a Timely Manner**

System Name	Disabling Period	Total	User Accounts	Non-User Accounts
COE LAN <sup>a</sup>	> 30 days	898	898	See Note a.
Volpe Center LAN	> 60 days	240	118	122
USMMA LAN <sup>b</sup>	> 60 days	258	189	69
FAA/ATO LAN	> 60 days	1,432	1,238	194
<b>Total</b>		<b>2,828</b>	<b>2,443</b>	<b>385</b>

Source: OIG

<sup>a</sup> User and non-user accounts were not segregated by COE.

<sup>b</sup> USMMA LAN store, process, and transmit PII.

The primary cause of these account problems is the inadequate use of tools that automatically disable accounts after a certain length of time of inactivity. The United States Maritime Marine Academy (USMMA) and John A. Volpe National Transportation Systems Center (Volpe) did not use any automated mechanism to disable its inactive accounts. Both COE LAN and FAA's ATO have implemented tools to manage their Active Directories that are not properly configured to disable accounts within the proper timeframes. Not disabling accounts in a timely manner may lead to unauthorized access to information and systems by individuals who are no longer authorized to have access.

<sup>20</sup> "Impact" refers to the impact that loss of a system's confidentiality, integrity, or availability could be expected to have on organizational operations, assets, or individuals. "High impact" would have a severe or catastrophic adverse effect, whereas "moderate impact" would have a severe adverse effect.



*Network Administrators Do Not Properly Distinguish Account Types*

NIST requires agencies to segregate account types (individual, group, system, application, guest/anonymous, or temporary), and distinguish account types between user and non-users. However, the networks we reviewed had not accomplished these requirements because their administrators did not follow the OAs' naming standards when establishing accounts. Table 11 provides examples of inconsistent account names among the networks reviewed. Without accurately identifying user accounts and non-user accounts, the Department cannot properly control access to its information systems.

**Table 11: Summary of Account Naming Errors**

Network	Account Naming Standard	Correctly Named Accounts	Incorrectly Named Accounts
COE	<i>Federal:</i> first.last	alan.walsh curtis.johnson	walsha Curtis.Johnson2
	<i>Contractors:</i> first.last.ctr	jean-marie.tchokok.ctr	j.tchokok.ctr
	<i>Naming convention for service accounts were not specified</i>	Unknown	Sptest SRS.Web DOTMOSS.Sql
FAA/ATO	<i>Service Accounts must contain "SRVC" in front of the account name.</i>	SRVC-BEuser SRVC-Backup SRVC-MCUser SRVC-ORDBackup	BEuser Backup MCUser ORDBackup
USMMA	<i>Midshipmen structure:</i> 2digityearLastNameFirstInitialMiddleInitial 10LastFM	07DiehIE 08BeIE 13HumeZA	diehle 08belle 13HUMEZA
	<i>Non-midshipmen structure:</i> LastNameFirstInitial LastF	AnthonyS VendittoJ LiG	anthons joanna.venditto li(contractor)

Source: OIG

### *The Department Has Not Implemented Multi-Factor Authentication for Identifying Users*

Department officials in charge of the four networks reviewed indicated that multi-factor authentication would not be implemented until they completed PIV card issuance. The Department agreed with OMB to complete card issuance by December 31, 2010. However, DOT's current plan to issue cards to non-FAA personnel lacks detail on issues such as resources, responsible parties, and risk management, without which the department cannot ensure that the timeframe is realistic. Currently, the four reviewed networks only use user IDs and passwords to allow access to their systems. USMMA is planning to implement multi-factor authentication for Federal employees and contractors, but not for midshipmen or four-year students, despite the fact that USMMA LAN stores, processes, and transmits PII. Because multi-factor authentication has not been implemented, the DOT cannot fully identify and authenticate authorized users. Individuals who are not properly authenticated may be capable of sharing user IDs and passwords which could lead to identity fraud, counterfeiting, organizational espionage, social engineering, Internet misuse, and misuse of personal information.

### *Not All Network Administrators Have Dual Accounts*

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 only use the user account to access email. Administrators of two of the networks we reviewed did not have user accounts. For example, COE administrators do not use separate accounts to perform non-administrator tasks. Because administrator accounts have greater access to computer resources, using such accounts to perform non-administrator functions increases the likelihood that malware, such as viruses, will infect DOT networks.

## **CONCLUSION**

DOT operates in a world in which information systems are part of every solution, and the Internet has connected almost every network. As a result, the Department's success is dependent on its ability to keep its networks available to its legitimate users, and to protect itself from those who, from almost any location, may seek to gain unauthorized access to its information or disrupt its operations. 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. To mature towards such a program, DOT must immediately address its persistent cybersecurity weaknesses with strong leadership, greater influence and oversight by DOT OCIO, and management

commitments from OA Administrators. Until this happens, DOT will continue to remain vulnerable to predators.

## **RECOMMENDATIONS**

Recognizing the challenges to develop an effective and mature information security program from what DOT has currently in place, we are providing a number of actions that, combined with our prior year recommendations, may serve as a roadmap to address urgent vulnerabilities currently inherent in the program. To mitigate these weaknesses and enable DOT's information security program evolution towards an appropriate level of maturity, we recommend that the Chief Information Officer do the following:

### **Information Security Policy:**

1. 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. To the extent the OAs require their own guidance, review guidance to verify compliance with department policies and procedures.

**Enterprise-Level Weaknesses:**

3. 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. 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. Require OST to implement required system patches on their Delphi system.
6. 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. Require and approve deviation requests for those non-conforming settings that are truly needed and for which risks have been mitigated and accepted.
8. Conduct periodic tests to assess FDCC compliance and deployment of patches, including service packs.
9. 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. Implement a practice to review OA specific incident handling procedures to ensure that they adhere to the departmental policy.
11. 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. 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. 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. Identify and implement automated tools to better track contractors and training requirements.

### **Information System Security Weaknesses:**

15. 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.

### **Information System Security:**

16. 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. Work with MARAD to finalize agreements with C&A service providers to certify MARAD systems.
18. Review the results of OA assessments to determine an accurate inventory of contractor systems.
19. 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. Research and standardize automated tools that will proactively monitor remote devices connecting to DOT networks.
21. Conduct tests of remote access solutions to ensure they comply with Federal requirements and DOT guidance.
22. 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. 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. Perform periodic reviews of active user accounts and network devices to identify accounts that need to be disabled.
25. Work with OAs to identify and logically segregate user accounts and service (role) accounts.
26. 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. Educate and assist OAs in implementing dual accounts for administrators. Subsequently, conduct reviews to determine that all DOT GSSs use these accounts.

## **MANAGEMENT COMMENTS**

A draft of this report was provided to the Department's CIO on November 3<sup>rd</sup>, 2010. On November 11<sup>th</sup>, 2010 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 Earl Hedges, Acting Assistant Inspector General for Financial and Information Technology Audits, at (410) 962-1729.

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 that we 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 April 21, 2010, the Office of Management and Budget (OMB) issued M-10-15, FY 2010, *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, which provides instructions for inspectors general for completing their FISMA evaluations and the required OMB template. For 2010, OMB has required the use of a common Web portal to upload its required metrics—a significant number of which have changed.

To meet FISMA and OMB requirements, we selected a representative subset of 33 departmental systems (see Table 12) and reviewed the compliance of these systems with NIST and OMB requirements in the areas of risk categorization, security plans, annual control testing, contingency planning, certification and accreditation, incident handling, and plans of actions and milestones. To evaluate FDCC compliance within the Department, 77 individuals within Washington area with government-provided computers were tested for Windows, Internet Explorer and Windows firewall compliance. We used a NIST-approved SCAP tool to perform these evaluations. Our sample of 77 individuals included 63 statistically-selected individuals, and all 14 individuals from the FMCSA remote site which was selected based on geographical location and is representative of FMCSA remote sites throughout the US.

In addition, for account and identity management, we reviewed four general support systems (GSS): (1) Common Operating Environment (COE) Local Area Network (LAN), (2) Volpe Center LAN, (3) U.S. Merchant Marine Academy (USMMA) LAN, and (4) Federal Aviation Administration/Air Traffic Organization (FAA/ATO) LAN. We also conducted testing to assess the Department's inventory, its overall process of resolving 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 Cyber Security Assessment and Management system, reviews of supporting documentation, and interviews with departmental officials. We also used commercial scanning software to assess compliance with Federal Desktop Core Configuration requirements.

## **Exhibit A. Scope and Methodology**

**Table 12: OIG's Representative Subset of DOT Systems**

<b>Operating Administration<sup>a</sup></b>	<b>System</b>	<b>Impact Level</b>	<b>Contractor System?</b>
FAA	110A (110A Inspector Credentials)	High	No
FAA	ANICS (Alaskan NAS Interfacility Communications System)	Moderate	No
FAA	ATOS (Air Transportation Oversight System)	High	No
FAA	BMX (Business Management Solutions)	Moderate	No
FAA	CMIS (Certificate Management Information System)	Low	No
FAA	CMRIS (Consolidated Management Resource Information System)	Low	No
FAA	CSMC Intrusion Detection Prevention System, IDPS (DR, NIDS, & WIDS)	Moderate	No
FAA	FDIO (Flight Data Input/Output)	Low	No
FAA	FPPS (Facility Power Panel System)	Low	No
FAA	FSIMS (Flight Standards Information Management System)	High	No
FAA	FSTNA (Flight Standards Training Needs Assessment)	Moderate	No
FAA	GIMS (GNAS Information Management System)	Low	No
FAA	LERIS (Labor and Employee Relations Information System)	Moderate	Yes
FAA	OPSS (Operations Specifications Sub-System)	High	No
FAA	SOAR (System of Airport Reporting)	Moderate	No
FHWA	Delphi Interface Maintenance System (DIMS)	High	No
FHWA	Knowledge Management	Moderate	No
FHWA	User Profile and Access Control System (UPACS)	High	No
FHWA	Video Conferencing System	Low	No
MARAD	Cadet Training Berthing System (CTBS)	Not Categorized	No
MARAD	Cargo Preference Overview System (CAPOS)	Not Categorized	No
MARAD	Credit Program Portfolio Management System (CPPMS)	Not Categorized	No
MARAD	MARAD Common Infrastructure (MCI)	Not Categorized	No
MARAD	MARAD Internet	Not Categorized	No
MARAD	Marine View (Marview)	Not Categorized	No

**Exhibit A. Scope and Methodology**



Operating Administration <sup>a</sup>	System	Impact Level	Contractor System?
MARAD	Virtual Office Acquisition (VOA)	Not Categorized	No
NHTSA	Mission Based Moderate Impact System <sup>b</sup>	Moderate	No
OST	Congressional Reporting Requirements Tracking System (CRRTS)	Low	No
OST	DELPHI	Moderate	No
RITA	Transtats	High	No

Source: OIG

<sup>a</sup> See Exhibit B for full Operating Administration names.

<sup>b</sup> NHTSA "Mission Based Moderate Impact System" is composed of 4 systems (GTS, VSH, MVII, CARSII) which increased the C&A sample systems reviewed from 30 to 33

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 DOT Operating Administrations, including OIG. In addition to preparing our submission, we reviewed the Department's progress in resolving weaknesses and implementing recommendations identified in our prior year's FISMA report.

We performed our information security review work between March 2010 and October 2010. We conducted our work at departmental and Operating Administration Headquarters offices in the Washington, D.C., area. 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 the FISMA legislative mandate (formerly the Government Information Security Reform Act) include:

## **Exhibit A. Scope and Methodology**

*Audit of DOT's Information Security Program and Practices*, FI-2010-023, November 18, 2009;  
*Audit of Information Security Program*, FI-2009-003, October 8, 2008;  
*Information Security Program*, FI-2008-001, October 10, 2007;  
*Information Security Program*, FI-2007-002, October 23, 2006;  
*Information Security Program*, FI-2006-002, October 7, 2005;  
*Information Security Program*, FI-2005-001, October 1, 2004;  
*Information Security Program*, FI-2003-086, September 25, 2003;  
*Information Security Program*, FI-2002-115, September 27, 2002; and  
*Information Security Program*, FI-2001-090, September 7, 2001.

## EXHIBIT B. DOT OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Operating Administration <sup>a</sup>	FY 2010	FY 2009
Federal Aviation Administration (FAA)	290	274
Federal Highway Administration (FHWA)	22	21
Federal Motor Carrier Safety Administration (FMCSA)	21	21
Federal Railroad Administration (FRA)	13	12
Federal Transit Administration (FTA)	5	5
Maritime Administration (MARAD)	21	10
National Highway Traffic Safety Administration (NHTSA)	11	10
Office of Inspector General (OIG)	2	2
Office of the Secretary (OST)	33	36
Pipeline and Hazardous Materials Safety Administration (PHMSA)	6	5
Research and Innovative Technology Administration (RITA)	13	10
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)	2	2
<b>Total Systems</b>	<b>440</b>	<b>409</b>

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

<sup>a</sup> For purposes of reporting under FISMA, we consider "Operating Administrations" to include all components listed above.

## EXHIBIT C. Status of Prior Year's Recommendations

<b>Recommendation Number</b>	<b>FY 2009 Recommendation</b>	<b>Status</b>
1	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	Open
2	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.	Open
3	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.	Open
4	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.	Open
5	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.	Open
6	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.	Closed
7	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.	Open
8	Use automated tools to periodically verify status of completion reported by Operating Administrations and identify deviations from the approved baseline configurations.	Open

Recommendation Number	FY 2009 Recommendation	Status
9	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.	Open
10	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.	Open
11	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.	Open
12	Develop and establish a tracking system that effectively and routinely accounts for all active contractors requiring security awareness training.	Open
13	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.	Open
14	Identify and ensure all employees with significant security responsibilities take the necessary specialized security training to fulfill their responsibilities.	Open
15	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.	Open
16	Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.	Open
17	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.	Open
18	Ensure that Maritime Administration properly inventories its information systems and tracks them in the Cyber Security Assessment and Management system. <b>(MARAD)</b>	Open
19	Ensure that Maritime Administration certifies and accredits each system in the revised inventory. <b>(MARAD)</b>	Open

### Exhibit C. Status of Prior Year's Recommendations

<b>Recommendation Number</b>	<b>FY 2009 Recommendation</b>	<b>Status</b>
20	Improve its quality assurance checks on the Operating Administrations' certifications and accreditations by increasing the frequency and scope of its checks, communicating results and expected actions to the Operating Administrations, requiring updated plan of actions and milestones to address weaknesses noted (including those found in the Inspector General reviews), and follow-up on resolution of weaknesses noted.	Open
21	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.	Open
22	Develop a process to ensure Operating Administrations continuously monitor and test information system security controls.	Open
23	Finalize the inventory count for systems containing privacy information.	Closed
24	Work with Operating Administrations to complete privacy impact assessments for applicable information systems.	Open
25	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.	Open
26	Implement 2-factor authentication for remote access.	Open
27	Implement NIST-approved encryption on all mobile computers/devices.	Open

Source: OIG

## Exhibit C. Status of Prior Year's Recommendations

**EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT**

<b><u>Name</u></b>	<b><u>Title</u></b>
Louis C. King	Program Director
Michael Marshlick	Project Manager
Lissette Mercado	Project Manager
Martha Morrobel	Information Technology Specialist
James Mullen	Information Technology Specialist
Tim Roberts	Information Technology Specialist
Tracy Colligan	Information Technology Specialist
Petra Swartzlander	Statistician
Susan Neill	Writer-Editor


## APPENDIX. MANAGEMENT COMMENTS

---

### Memorandum

Date: November 10, 2010

To: Calvin L. Scovel III, DOT Inspector General

From: Nitin Pradhan, DOT Chief Information Officer (CIO) 

Prepared by: Andrew Orndorff, DOT Chief Information Security Officer (CISO)

Subject: DOT CIO Response to OIG Report: Timely Actions Needed to Improve DOT's Cybersecurity, **Project Number: 10F3012F000**

---

#### **DOT Taking a Fresh Approach to Improve Cyber Security**

New cyber security threats require federated technology-based environments, like the Department of Transportation (DOT), to update its methods for monitoring networks, detecting potential risks, identifying malicious activity and mitigating threats to protect information systems. We have recognized the need for cyber defenses to evolve quickly and continuously along both strategic and tactical lines while new capabilities are brought online to keep pace with ever more sophisticated and well-funded threats. These threats evolve rapidly and are no longer addressed well by the static, discrete solutions of just a few months ago, let alone those that evolved in the early 21<sup>st</sup> century. In order to address today's cyber security threats, the Department has initiated a paradigm shift from a reactive, gradual and segmented cyber security approach to a new holistic, predictive, proactive, rapid and agile process that is responsive to the evolving cyber threats matrix.

#### **DOT Initiated Implementation of a New Cyber Security Framework**

The DOT Office of the Chief Information Officer (OCIO), working with the operating administration (OA) CIOs and system owners, the Department of Homeland Security (DHS), the National Security Agency (NSA), and other major industry and academic partners is preparing to implement a next generation approach to achieve the cyber security goals outlined by the Administration. This approach to cyber security is intended to be more agile, proactive and predictive and will be strengthened by closer collaboration and information sharing among core communities including government intelligence,



cyber crime law enforcement, IT cyber security and private sector experts. This process enables DOT to constantly weigh the operational and tactical activities against the DOT strategic roadmap to deliver the best cyber security environment within its resources.

As part of this framework, DOT is focused on establishing a comprehensive foundation of strategies, plans, metrics, oversight and reporting necessary to improve cyber security and better measure our effectiveness. The framework includes three primary elements:

- Tactical - based on realistic and straightforward actionable items
- Strategic - based on foundational and transformational capacity
- Compliance - based on existing rules, regulations and compliance requirements

***Tactical - DOT Cyber Security Assessed through Vigorous Real World Tests***

For the first time, the Department engaged the foremost experts in cyber security at the National Security Agency (NSA) to perform an objective, independent, technical assessment of the Department's IT security against realistic known and active threats as part of a tactical proactive approach. The outcome of this testing was a report with detailed information on the security posture of our networks. The CIO's Office used this information to develop prioritized actions addressing the most critical vulnerabilities first. The tactical element flows from its recognition of and operation within existing resource limitations to address areas of greatest risk to DOT, and is directly integrated within the strategic approach and resource planning requirements. In order to ensure critical testing is institutionalized, DOT plans to create an independent team for ongoing future assessments, subject to resource availability, via the FY 2011 budget. Finally, the CIO's Office will continue to provide weekly briefings to the Deputy Secretary to appraise top management of the Department's progress addressing these evolving real-world challenges.

***Strategic - DOT Strategy Identifies Resources, Processes, and Investment Approach***

DOT is one of the first major agencies to develop a holistic cyber security plan that invests in people, process and technologies in six focus areas: human capital planning and training, consolidation and integration, cyber situational awareness and remediation, infrastructure planning and upgrade, business value and governance, and critical transportation infrastructure protection.

Throughout FY2010, DOT focused on the development and implementation of the Transportation Cyber Security Strategic Plan as a necessary and critical foundation for the DOT cyber security program. Prior administrations attempted to address FISMA performance through short term redirection, or by addressing immediate audit findings, without addressing the systemic issues limiting and impacting agency program performance. Unfortunately, while these types of patchwork actions are intended to improve FISMA metrics scores, simple adherence to improving FISMA metrics has been insufficient, in itself, for significant improvement to the Department's cyber security posture.

Our strategic approach relies on a number of key elements to improve cyber security while producing discernable improvement in FISMA metrics. First, we have prepared a detailed and credible strategic plan, linking program performance to the budget and capital planning processes through investment exhibits and the IRB. We are also actively advocating for necessary resources before OMB and Congress. These efforts are intended to ensure that foundational strategic requirements are in place to expand our tactical cyber threat response. It will also enable us to more completely address the compliance activities and specific FISMA metrics. By aligning with Federal initiatives and documenting a path forward for program enhancement and sustainment, the strategic plan links these concepts—strategic planning, operational responsiveness, tactical awareness, resources, personnel, processes, policies and technology—together into a comprehensive intermodal action plan. DOT leadership has provided significant support to the Cyber Security Strategic Plan and is measuring results to objectively determine progress and provide oversight. The OAs have also used the plan to identify and address individual metrics in cyber security. The plan further underscores the Department's emphasis on security awareness, planning, program sustainment and outreach to stakeholders like the transportation sector.

Executing the Strategic Cyber Security Plan relies heavily on DOT making critical investments in both human resources and infrastructure. We are focused on hiring highly skilled and fully qualified personnel adept at best practices so their actions can provide maximum achievable value to the Department. Similarly, we need to make judicious investments in IT infrastructure that are targeted towards critical vulnerabilities and aligned with the mission and business of DOT. Using this balanced approach of leveraging high-quality people and careful investment in infrastructure, DOT expects to improve its posture and reduce cyber security risks.

**Compliance - With Strategy in Place, Compliance Elements Will Receive Increased Focus**

DOT recognizes that FISMA has an important role in improving security by focusing on information systems inventory, risk, system security plans, certification and accreditation, and continuous monitoring. However, the numerous tactical elements included in FISMA are not prioritized, nor is there explicit recognition of resource constraints that factor into the extent to which individual agencies may comply with each of its requirements. DOT is working through the changes to FISMA and is focused on retooling existing capabilities and planning for future capacity to address its cyber security needs. Additionally, DOT is exploring changes in internal processes to allow for speedy rollout of new DOT-wide policies, procedures and recommendations. While we have focused significant resources on improving cyber security from a holistic perspective in 2010, these efforts, being primarily longer term in nature, are not necessarily directly reflected in the 2010 FISMA metrics.

While compliance requirements like FISMA are an important part of the overall cyber security program, the Department considers all aspects of cyber security when determining how to distribute its limited resources. For example, in order to fully comply with FISMA certification and accreditation requirements, the Department would need to more than triple its information security workforce. As a result, the Department must prioritize its efforts to focus on actions which offer the greatest potential cyber security benefit. With our strategic plans in focus, DOT will be able to devote appropriate resources to the individual compliance elements, including FISMA metrics.

**DOT Achieved Significant Cyber Security Progress in 2010**

Thanks to the extraordinary efforts of cyber security and support professionals across the Department, we achieved a number of key accomplishments during the past year. While not fully reflected in the OIG report, these include

- **Increased Cyber Security Resources** - The Department included in the President's budget request funding for IT capital and personnel resources in FY2011 to enhance the cyber security program.
- **Improved Cyber Security Training** - A tip-of-the-day continuous training solution was piloted to improve the performance and relevance of awareness training for departmental personnel. The new tool has the capability to deliver specialized content based on an employee's role and responsibilities, and to incorporate training elements other than cyber security and privacy. This

tool is scheduled to be rolled out across the Department with the availability of our FY 2011 appropriation.

- **Cyber Security Awareness Briefings** - The Department initiated, for the first time ever, documented threat awareness briefings to leadership to increase cyber security awareness and support for cyber initiatives throughout the Department. This was followed up with several enterprise-wide cyber security awareness campaigns including posters, articles and awards.
- **Infrastructure Upgrades** - The Department has implemented plans to upgrade critical IT components. DOT will begin implementing Windows 7 during calendar year 2011, which enhances the security of desktop configurations and addresses a major finding the Department's voluntary National Security Agency (NSA) FY10 Vulnerability Assessment. The Department's investment in the Identity, Credential, and Access Management (ICAM) program in FY10, which currently enables multi-factor authentication across the agency, is also expanding as more employees begin to use their Personal Identity Verification (PIV) cards to gain logical access to information systems.
- **Reprioritized and Reprogrammed Existing Resources** - The Department reprioritized discretionary contract funds to facilitate hiring of personnel necessary for the enhancement and sustainment of cyber security oversight and operational functions. Recruiting is actively underway to fill the positions with qualified personnel now that the Department, OPM, Congress and other entities have approved.
- **Improved Cyber security Data Tracking** - The Department upgraded the Cyber Security Assessment and Management (CSAM) Security Management System to provide advanced reporting and dashboards for integration into the DHS Cyber Scope system, enabling greater departmental oversight and transparency. In addition, DOT is one of the few Federal agencies that implemented the use of the Department of Homeland Security's (DHS) Cyber Scope system early, including requiring all involved Department and component personnel to acquire the necessary credentials to obtain system access, establishing the Department as a leader in the integration into and participation in the Federal risk management process.
- **Improved IT System Inventory** - The Department, for the first time ever, rationalized its investment and system inventories, reconciling with component-level budgets to comprehensively identify all systems and assets while establishing traceability between information technology expenditures and operational systems. In the process, the Department

identified expenditures for systems that were not being tracked and ensured that departmental system owners were properly reporting security and information technology costs.

- **Enhanced Business Processes** – The Department developed a new records management program with a focus on identifying and cataloging agency information for preservation and protection, as well as an integrated project management methodology aiming to institutionalize disciplined project management that incorporates Federal and industry best practices. This will ensure that full investment life cycle requirements, including cyber security, are incorporated into every new initiative.
- **Implemented Technology Test and Evaluation Capability** - The Department for the first time has established a fully functional test environment for the identification, evaluation and assessment (including security design validation) of new and emerging technologies; determining the relevance of new technologies for DOT; and integrating new technologies into the DOT Common Operating Environment (COE) architecture and infrastructure for increased business value, functionality and security.
- **Strengthened Transparency and Governance** - The Department for the first time has a complete, functioning governance structure including the DOT-wide investment review board, the CIO Council and the Core CIO meeting, the new Technology Control Board and the new Technology Council, and finally the Cyber Security and Privacy Council.

Work on these accomplishments continues, within current resources, in addition to other federally mandated initiatives including data center consolidation and the trusted Internet connection program.

The Department is proud of its cyber security accomplishments and its demonstrated commitment to enhance cyber security throughout FY2010. Significant change has occurred, however—we recognize that much more remains to be accomplished. We look forward to working with all our stakeholders to further strengthen and improve DOT’s cyber security program throughout FY11.

#### **OIG Recommendations and Responses**

The Department will be happy to provide specific and detailed responses to the OIG recommendations as enumerated in the final report.