AUDIT OF DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES

Department of Transportation

Report Number: FI–2010–023
Date Issued: November 18, 2009

Memorandum

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

Subject: ACTION: Audit of Information Security Program, Department of Transportation
Report Number: FI-2010-023

Date: November 18, 2009

From: Calvin L. Scovel III
Inspector General

Reply to Attn. of: JA–20

To: Chief Information Officer

The Department of Transportation's (DOT) annual $3 billion information technology (IT) portfolio is one of the largest among the Federal civilian agencies. DOT's IT budget currently covers more than 400 information systems across 13 Operating Administrations—nearly two-thirds of which belong to the Federal Aviation Administration (FAA). DOT's financial systems manage and disburse over $50 billion in Federal funds each year.

In May 2009, the White House reported on the urgent need to secure the Nation's digital infrastructure from individuals who compromise, steal, change, or destroy information vital to our economy and national security.[1] To protect information and information systems that support Federal operations and assets from such 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 agency's information security program 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, (2) enterprise level information security controls, (3) management of known information security weaknesses, (4) system level security controls, and (5) controls over privacy related information. As required by OMB, we also provided various assessments and performance measures to OMB via its Web portal.[2]

[1] White House Report on Cyberspace Policy Review, May 2009.
[2] OMB has designated this information as "For Official Use Only." Consequently, our submission to OMB is not contained in this report.

To conduct our work, we selected a representative subset of 45 departmental systems and reviewed their compliance with National Institute of Standards and Technology (NIST) and OMB requirements in seven areas: risk categorization, security plans, annual control testing, contingency planning, certification and accreditation, incident reporting, and plan of actions and milestones. We also conducted testing to assess the Department's inventory of systems, its overall process of resolving information security weaknesses, certain privacy requirements, configuration management, incident reporting, and security-awareness training. 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 (FDCC) requirements. Our audit was conducted in accordance with generally accepted government auditing standards. See Exhibit A for more details on our scope and methodology.

RESULTS IN BRIEF

During fiscal year 2009, DOT made notable improvements in two key areas. First, the Department's Office of the Chief Information Officer (OCIO) completed and issued its long-awaited information security policy that was required by FISMA in 2002—the first step in building a sustainable information security program. This much-needed policy addressed all of NIST's 17 information security control areas. Second, DOT significantly improved its Common Operating Environment's compliance with FDCC, which prescribes secure settings for Windows XP software.[3] These actions are consistent with those recommended in our October 2008 report.[4]

Despite these accomplishments, the Department has not made the progress needed to address other critical areas. As a result, the departmental information security program is not as effective as it should be, and is non-compliant with all key FISMA and OMB requirements. We noted weaknesses in five critical areas:

- First, the OCIO's security policy lacks key elements, such as identifying staff that require specialized training to understand system security risks and their role in mitigating those risks. Such omissions contributed to other deficiencies we identified.
- Second, the Department has not demonstrated sufficient progress in implementing enterprise-level controls. Specifically, not all of its operating

[3] The Common Operating Environment provides network infrastructure support to DOT Headquarters and remote offices, except FAA.

[4] *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.

systems and database systems have security baseline configurations; the Department has no confirmation that all major security incidents reported to the Department of Homeland Security were received; and it has not provided essential security training to all employees and contract staff.

- Third, the Department has not effectively identified, tracked, or prioritized information security weaknesses to efficiently resolve these weaknesses. Of the approximately 5,400 DOT weaknesses that were tracked, about 1,000 were not remediated in a timely manner. Further, about 300 were not assigned a priority level and 2,400 lacked an estimated cost for remediation.
- Fourth, DOT has not provided adequate controls to protect or recover its systems and system interfaces in the event of a disruption. For example, DOT has not fully inventoried its system interfaces—including 18 e-Government initiatives, such as e-Payroll—with external systems, and could not provide security agreements for interfaces. Further, of the 45 DOT systems we reviewed, we found that half were not appropriately certified and accredited, did not have tested contingency plans, or both.
- Last, the Department has not fully protected privacy related information. DOT lacks an accurate count of systems that are privacy related and did not complete privacy impact assessments for at least 40 percent of these systems. In addition, DOT has not made significant progress in meeting OMB's requirement to reduce the use of social security numbers (SSN) by November 2009. FAA alone does not plan to satisfy this requirement until 2015. Finally, DOT has not used sufficient authentication and encryption procedures to control remote users' access to its networks.

To assist the agency in establishing and sustaining an effective information security program—one that complies with FISMA, OMB, and NIST requirements—we are making a series of recommendations, beginning on page 16. A draft of this report was provided to the Department's CIO on November 9, 2009. On November 16, 2009 we received the CIO's response, which can be found in its entirety in the Appendix. The CIO generally concurred with our findings and recommendations and in 30 days will provide written comments describing the actions and milestones that will be taken to implement the recommendations.

BACKGROUND

Ensuring a secure global digital information and communications infrastructure is one of the President's seven guiding principles in protecting the American people.[5] The White House subsequently reported that the Federal Government, as

[5] White House Issues: Homeland Security (www.whitehouse.gov/issues/homeland-security).

well as the private sector, is facing new cyber security threats. These threats include terrorists and international crime groups who are targeting U.S. citizens, commerce, critical infrastructure, and Government in order to steal, change, or destroy information. Undeterred, these individuals have the potential to undermine national security, degrade civil liberties protections, and even cripple society.

In October 2008, we reported that the Department's information security program and practices did not effectively safeguard DOT's IT systems and information. Specifically, we found that DOT had not established adequate policies, procedures, and training to identify information-security weaknesses and protect or recover computer systems and networks, including those with personally identifiable information (PII). We made 27 specific recommendations aimed at addressing these deficiencies. (See Exhibit C for a list of our recommendations and their implementation status.)

DOT'S INFORMATION SECURITY POLICY LACKS KEY ELEMENTS

FISMA requires the Chief Information Officer to develop and maintain information security policies, procedures, and control techniques to address security requirements. In fiscal year 2009, the Department issued a series of 19 information security policies. However, the policies lack critical elements to effectively and adequately guide the agency's information security program (see Table 1). The lack of an adequate policy increases the likelihood that Operating Administrations will create internal practices and ad-hoc procedures, which may not comply with OMB or DOT requirements. The deficiencies in DOT's information security policies have also contributed to the other weaknesses documented in this report.

Table 1: Examples of Information Security Policy Deficiencies by Program Area

Description	OIG Policy Evaluation
Incident Reporting	
Detecting, reporting, and responding to security incidents, including notifying law enforcement agencies and relevant OIGs.	The policy does not document the requirement to report incidents to law enforcement and OIG as required by FISMA and OMB.
Plans of Action and Milestones	
The POA&M tracks the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities.	The policy does not specifically identify the required data elements to properly document and report on information systems' or programs' security weaknesses throughout the lifecycle as required by OMB. Such information includes: Description of Weaknesses, Scheduled Completion Date, Key Milestones with Completion Dates, Milestone Changes, Source (e.g., program review, IG audit, GAO audit, etc.), and Status.
Security Training	
Disseminate security information that the workforce, both employees and contractors, need to do their job.	The policy does not address the identification of users with login privileges to the Department information systems. In addition, it does not identify specific job functions that require specialized security training, such as CIO, ISSO, Database Administrator, etc.
Contractor Oversight	
Monitor the effectiveness of security for systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.	The policy does not contain contractor oversight provisions that would ensure that proper security for the contracted information and systems are in adherence with NIST, OMB, and FISMA requirements.
External Interfaces	
Enforces System Interconnection/Information Sharing and Interconnection Security Agreement, Memorandum of Understanding, or Memorandum of Agreement between systems that share data that are owned or operated by different organizations.	The policy does not provide any guidance on the preparation of these critical interface agreements nor does it address key elements of NIST guidance.

Source: OIG Analysis

ENTERPRISE-LEVEL CONTROLS WERE INADEQUATE

Enterprise-level controls are controls that are implemented throughout the entire organization or infrastructure, such as configuration management, reporting of security incidents, and security training. While DOT has made significant progress in implementing security baseline configurations for Windows XP operating systems in the Common Operating Environment, it has not demonstrated

sufficient progress for other operating systems and databases. In addition, the Department has not provided evidence that all security incidents, including those that potentially breach PII, were reported to the Department of Homeland Security. Furthermore, while DOT has reported improvement to the number of employees receiving security awareness training, it still cannot provide evidence that all users received the training, including those requiring specialized security training.

Baseline Configuration Standards Have Not Been Fully Implemented

FISMA requires compliance with minimally acceptable system configuration requirements for commercial software. Common security configurations provide a baseline level of security and ensure efficient use of resources. To meet this FISMA requirement, the Department requested Operating Administrations to submit their configuration baseline and evidence of implementation. While all but three Operating Administrations have begun implementation, including scanning their systems to assess compliance, their scanning results indicated a significant amount of noncompliance needs to be remediated. Moreover, the three Operating Administrations that have not provided evidence of implementation—FAA, PHMSA, and SLSDC—together account for 68 percent of systems.

Without complete implementation of baseline configuration standards, the Department has little assurance that its information systems are sufficiently protected from known, exploitable weaknesses in key software. Inadequately configured software also increases security vulnerabilities, which could impact DOT's mission and business operations. In our May 2009 report on Web security, we noted that the inadequate configuration of Web applications contributed to hackers (1) compromising an FAA Web site to access an internal server, and (2) taking over FAA computers in Alaska.[6]

To meet OMB requirements for system configuration, DOT Acquisition Policy Letter APL-2007-01 states that contracting officers should include clauses in all IT solicitations requiring compliance with Federal security standards for Windows XP and Vista software no later than August 7, 2007. During our review, we found no evidence in FAA's Acquisition Management System (AMS) or DOT's PRISM system contracts that the required acquisition language on common security configurations was being incorporated. Without this language, DOT cannot ensure efficiency and security of its overall IT operations and implementation of security controls on DOT systems.

---

[6] *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, OIG Report FI-2009-049, May 4, 2009. OIG reports and testimonies can be found on our Web site at www.oig.dot.gov.

The Department Lacks Assurance that All Security Incidents Were Reported to US-CERT

According to DOT, when a security incident is logged, it is automatically reported to the United States Computer Emergency Readiness Team (US-CERT), and a reference number is generated for the security incident. Between July 1, 2008, and June 30, 2009, DOT had a total of 2,049 confirmed security incidents that needed to be reported to US-CERT. Yet 743, or 36 percent, of the security incidents did not have a US-CERT reference number recorded in DOT's incident logging system (see Table 2). Among these incidents, 107 security incidents pertained to potential or confirmed PII breaches and should have been reported within 1 hour. Without US-CERT reference numbers, DOT cannot determine if the Department of Homeland Security received this information, undermining the Government's ability to properly coordinate among Federal agencies to defend against cyber attacks.

Table 2: Summary of Incidents Missing US-CERT Reference Numbers

US-CERT Category[a]	Incidents Missing Reference Numbers	Percentage
Category 1: Unauthorized Access (e.g., PII breach)	107	14
Category 2: Denial of Service (DOS)	0	0
Category 3: Malicious Code	393	53
Category 4: Improper Usage	170	23
Category 5: Scans/Probes/Attempted Access	73	10
Total Security Incidents	**743**	**100**

Source: OIG Analysis

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

The Department Cannot Identify All Contract Personnel for Security Awareness Training and All Personnel Requiring Specialized Security Training

Security Awareness Training

NIST guidance calls for building and maintaining a comprehensive security awareness and training program that ensures all users are sufficiently trained in their security responsibilities and how to fulfill them before allowing them access to DOT information systems.[7] DOT training policy requires that all DOT Line of Business and Operating Administration (LoB/OA) CIOs ensure basic security

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

awareness training is provided to all DOT information system users before authorizing access to the system, upon system changes, and at least annually thereafter.

While most of the 57,000 DOT employees have received security awareness training, the Department could not ensure that all contractors with login privileges had completed the annual security awareness training because the various sources of information pertaining to contractor staff could not be reconciled. The Department reported that approximately 14,000 contractor staff were given access to DOT networks. Using data from the Cyber Security Assessment and Management (CSAM) system—the Department's information security reporting system—we estimated that about 11,000 contractor staff were trained during the reporting period. However, various training systems showed that about 27,000 contractor staff—almost twice the number of contractor staff DOT reported—were trained. Until the Department can accurately track contractor staff and users of DOT networks, it has no assurance that security awareness training is provided to all people who require it.

Specialized Security Training

DOT policy requires Operating Administrations to determine the appropriate content of specialized security training based on the specific requirements of their organization and systems that employees and contractors have access to. It also requires Operating Administrations to provide to system owners, system and network administrators, and other personnel having access to system-level software with adequate specialized security training to perform their assigned duties.

However, not all employees with significant security responsibilities are receiving specialized security training. The Department reported 884 employees with significant security responsibilities. This number did not include approximately 63 in nine Operating Administrations—including nine OA Chief Information Officers—who should have received specialized training. Our estimate was based on eight job functions that require specialized training as documented by NIST 800-16. The job functions included Chief Information Officer, Security Officer, System Administrator, System Developers, Network Administrator, Database Administrator, System Certifier, and Designated Authorizing Authority (DAA) (see Table 3).

Table 3: Unreported Job Functions & Estimated Employees Requiring Specialized Training

Unreported Categories	FRA	FTA	MARAD	NHTSA	OIG	OST	RITA	SLSDC	STB	Total Unreported
Chief Information Officer	1	1	1	1	1	1	1	1	1	**9**
ISSO/ISSM		1				1		1	1	**4**
System Administrator	1	1	1	1		1	1	1	1	**8**
System Designer/Developers	1	1	1	1	1	1	1	1	1	**9**
Network Administrator	1	1	1	1		1	1	1	1	**8**
Database Administrator	1	1	1	1	1	1	1	1	1	**9**
System Certifier	1	1	1	1		1	1	1	1	**8**
Designated Authorizing Authority	1	1	1	1		1	1	1	1	**8**
Total Unreported	**7**	**8**	**7**	**7**	**3**	**8**	**7**	**8**	**8**	**63**

Source: OIG Analysis

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

Personnel in other job functions also have access to system level software and, therefore, require specialized training. OIG IT management is in the process of evaluating which OIG staff requires specialized security training. To date, it has reported to the OCIO that at least 13 others, in addition to the three identified in the table and the one reported earlier to OCIO, require some degree of specialized training. As a result of not adequately identifying those employees with significant security responsibilities and providing them with the required specialized training, these employees may not have the correct skill set needed to perform their security responsibilities. Consequently, Department information systems are at risk of not appropriately securing the information and information systems.

THE DEPARTMENT LACKS AN EFFECTIVE PROCESS TO REMEDIATE INFORMATION SECURITY WEAKNESSES

FISMA requirements for agency information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address information security weaknesses. However, the department process is not effective. Key concerns are weaknesses in management oversight and reporting of open security weaknesses.

Management Oversight Approach Is Ineffective

In February 2009, the DOT OCIO began meeting monthly with Operating Administrations to address information security concerns. Despite these meetings, the percentage of overdue items increased from 13 percent to 17 percent over the past year. There were also a significant number of items that had been overdue for more than one year—a total of 351 items. Almost 95 percent of these items came from DOT Programs, FHWA, PHMSA, and STB (see Table 4).

Table 4: Summary of Overdue POA&Ms

Operating Administration[a]	Total Open POA&Ms	1 - 60 days	61 - 90 days	91 - 120 days	121 days - 1 year	> 1 yr	Total Overdue	No Target Completion Date	Future Scheduled Completion Date
DOT Programs	69	0	0	0	1	**64**	65	1	3
FAA	4,397	148	34	14	56	9	261	7	4,129
FHWA	514	52	0	1	73	**89**	215	0	299
FMCSA	3	0	0	0	0	2	2	0	1
FRA	20	20	0	0	0	0	20	0	0
FTA	50	5	7	0	23	0	35	0	15
MARAD	0	0	0	0	0	0	0	0	0
NHTSA	7	0	0	0	0	6	6	0	1
OIG	18	2	2	2	8	0	14	2	2
OST	149	10	0	127	0	0	137	1	11
PHMSA	128	0	0	0	0	**128**	128	0	0
RITA	19	0	0	0	0	1	1	18	0
SLSDC	1	0	0	0	0	0	0	1	0
STB	67	0	0	0	0	**52**	52	15	0
Total	**5,442**	**237**	**43**	**144**	**161**	**351**	**936**	**45**	**4,461**
Percentage		**4%**	**1%**	**3%**	**3%**	**6%**	**17%**	**1%**	**82%**

Source: DOT Open POA&Ms in CSAM as of July 15, 2009

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

Operating Administrations did not meet Department requirements for addressing security weaknesses. Specifically, Operating Administrations did not do the following:

- Assign a priority and the time for remediation within the allowed time constraints—high-priority (24 hours), moderate-priority (20 working days), and low-priority (about 3 months)—to 395 security weaknesses, 330 of which were for systems or programs categorized as "High" and "Moderate" to the mission of the Department.
- Establish target completion dates for 45 items or target completion dates within the maximum time allowed by policy for 2,635 out of 4,461 items. Of the 2,635, 64 security weaknesses are not scheduled for remediation until 2015.
- Estimate costs needed to fix 2,393 items out 5,442.

In addition, Operating Administrations did not record all identified security weaknesses in the plan of action and milestones (POA&M) database for 32 of the 45 systems that we selected for review this year. In particular, MARAD did not input any known security weaknesses in the POA&M database.

Management Reporting Is Unreliable

We found significant discrepancies between the POA&M database and the Security and Privacy Posture Summary Status Report, dated July 2, 2009, used by the CIO office to monitor Operating Administrations' progress in correcting identified security weaknesses (see Table 5).

Table 5: OIG POA&M Data Analysis Comparison Results

	OCIO's Report	POA&M Database	Difference
Total number of open POA&Ms	4,674	5,442	**768**
POAMs not categorized	247	395	**148**
Unidentified cost	0	2,393	**2,393**
Overdue POA&Ms	276	936	**660**

Source: CIO's Security and Privacy Posture Summary Status Report dated July 2, 2009 and DOT Open POA&Ms in CSAM as of July 15, 2009

Without proper management of a compliant POA&M process, there is little assurance that its systems are adequately secured and protected. Specifically, without documenting security weaknesses, estimating cost, prioritizing risk, or updating milestones such as scheduled completion dates to resolve or mitigate all weaknesses, it is difficult or impossible for the Department and the Operating Administrations to adequately prioritize and resolve open weaknesses. As a result, weaknesses of lesser urgency may get resolved before critical ones. In addition, allowing weaknesses to remain unaccounted, unresolved or unmitigated for extended periods increases the risk that such vulnerabilities and exposures may be exploited by intruders, or may otherwise compromise the confidentiality, availability or integrity of systems and data.

SYSTEMS ARE NOT ADEQUATELY PROTECTED OR TESTED TO ENSURE RECOVERY

The Department continues to lack an accurate and complete inventory of its information systems and related interfaces and a process to ensure system owners have complete information to approve systems. Without such information, DOT cannot ensure its information systems are protected or can be recovered.

Specifically, DOT does not have an inventory of system interfaces, including 18 e-Government initiatives, with external systems and could not provide security agreements for interfaces. In addition, MARAD did not inventory systems correctly and did not perform adequate security testing to ensure protection of sensitive information. Of the 45 DOT systems reviewed, we found that half were not appropriately certified and accredited, did not have tested contingency plans, or both.

The Department's Inventories of MARAD Systems and External System Interfaces Are Not Comprehensive

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. These inventories are used to track agency systems for annual testing and evaluation and contingency planning. As such, a complete and accurate inventory of major information systems is the first step in managing the agency's information technology resources, including the security of those resources. Further, OMB requires an Interconnection Security Agreement, Memorandum of Understanding, or Memorandum of Agreement between systems that share data and are owned or operated by different organizations.

DOT had no major weaknesses in accounting for its internal systems. However, MARAD did not use an appropriate methodology to develop its system inventory. MARAD classified 35 of its applications as minor and then proceeded to group them into eight different systems for certification and accreditation. The systems contained unrelated applications that did not comprise a system boundary suitable for certification and accreditation. As a result of inappropriate system grouping, component applications did not receive proper security review. For example, one system had five applications; however, there is no evidence that two applications were reviewed as part of the certification and accreditation process. Without a well developed inventory, it is almost impossible to determine if system-level controls are implemented or effective, or to track security metrics for systems. In addition, as changes occur to systems, it is difficult to reassess system level controls or to enforce security at the system level.

While the Department could generally account for its internal systems, it was unable to provide a list of all interfaces with external systems. For example, 18 e-Government initiatives, including e-Payroll and GovTrip, were not included in the inventory. Also, the Department could not provide required security agreements for those interfaces. Without an accurate inventory of interfaces, the Department cannot ensure that the interfaces are being managed properly or that the information transmitted over these interfaces is secured.

Certification and Accreditation and Contingency Plan Testing Are Not Adequate

FISMA requires agencies to report on their certification and accreditation of systems—a process to formally evaluate (certify) the management, operational, and technical controls established in an information system's security plan and authorize (accredit) the systems for operation. However, DOT's certification and accreditation process does not provide complete information to support risk-based decisions or ensure that security controls are updated or tested on a periodic basis.

Of the 45 DOT systems we reviewed, 25 were not compliant with the certification and accreditation standards in NIST 800-37 (see Table 6). Specifically, Operating Administrations were deficient in performing risk categorizations and assessments, security control selection and testing, and contingency plan testing. We also found that nine of the 45 systems (20 percent) did not test controls in the last 12 months, as required by OMB.[8] In addition, 22 of the 45 did not have tested contingency plans.

Incomplete or inadequate system security assessments may result in the approval of operating systems that have risks. Such risks include exploitable vulnerabilities that result from missing or weak controls and inadequate security planning. In addition, without complete security and contingency testing, systems may be operating with critical new or unresolved weaknesses and risk not being recovered in time to minimize business disruption.

[8] OMB requires agencies to test a subset of the security controls annually—as part of its continuous monitoring—subsequent to the initial authorization of the information system.

Table 6: Sample Systems Results Summary by Operating Administration

	FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OST	PHMSA	RITA	Total
Number of Systems Sampled	28	1	3	1	2	1	1	6	1	1	**45**
Systems without Fully Compliant C&As	22	0	0	0	0	1	0	2	0	0	**25**
Systems without Annual Testing	5	0	2	0	0	1	1	0	0	0	**9**
Systems without Tested Contingency Plans	16	1	0	1	0	1	0	2	1	0	**22**

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

PRIVACY PROTECTION PROGRAM STILL NOT MEETING OMB REQUIREMENTS

While the Department has made some progress in completing OMB privacy protection requirements, it lacks a reliable count of systems that are privacy related and did not complete privacy impact assessments for at least 40 percent of these systems. In addition, DOT has not implemented key privacy initiatives, including reducing the use of SSNs—a process which OMB required to be completed by November 2009—and using appropriate authentication or encryption for controlling remote access to its networks.

Count of Systems Containing Privacy Information Is Unreliable and Privacy Impact Analyses Are Incomplete

OMB policy established criteria and instructions for agencies to manage systems containing privacy information. Specifically, OMB policy requires agencies to (1) conduct privacy impact assessments for electronic information systems that collect identifiable information, (2) report annually to OMB on compliance with section 208 of the E-Government Act of 2002[9], and (3) submit completed assessments to OMB no later than October 3, 2003.

According to the Security and Privacy Posture Summary Status Report, DOT has not completed privacy impact assessments for at least 40 percent of the systems that require one (48 of 116)—almost six years after they were required. Without

[9] OMB requires agencies to address information technology systems or information collections for which PIAs were conducted, persistent tracking technology uses, agency achievement of goals for machine readability, and contact information of the person responsible for privacy policies.

completing all privacy impact assessments, the Department cannot fully ensure that private information collected is only used for its intended purpose and is not disseminated without individual consent and knowledge.

Conducting the assessments is problematic in part because DOT lacks an accurate count of its privacy systems. Last year, the Department reported that 109 systems contained PII. In September 2009, 140 systems in the Department's security database were identified as containing PII. However, the Security and Privacy Posture Summary Status Report showed a count of 201 PII systems, a discrepancy of about 60 systems. Without a valid inventory of systems that have privacy information, the agency has little assurance in the integrity of the privacy information reported or the confidentiality of PII contained in systems that may be missing from the inventory.

The Department Has Not Implemented Key Privacy Initiatives

The Department has also failed to fully implement three key OMB requirements to safeguard privacy-related information: reduce the use of SSNs, employ two-factor authentication, and encrypt mobile devices that contain PII (see Table 7). As a result, the Department cannot ensure that all PII is properly protected or minimize the risks that SSNs are exposed to parties who do not have a legitimate need to know or possess them.

Table 7: DOT Implementation of OMB Privacy Initiatives

OMB Initiative	Status
Complete SSN reduction and PII volume reduction.	DOT identified 25 systems that can reduce use of SSNs. Only 5 systems have completed a plan to do so. In addition, FAA does not plan to eliminate unnecessary use of SSNs until 2015.
Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.	Two-factor authentication delayed until DOT implements Homeland Security Presidential Directive 12.
Ensure that all PII data stored or carried on mobile computers/ devices is encrypted using NIST-approved encryption.	As of July 2, 2009, 592 out of 11,723 mobile devices from the Department have not had NIST approved encryption applied. (No data were available for FAA and FHWA[a])

Source: OIG Analysis

[a] OMB requires encryption on any device used to store information that can be physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants).

CONCLUSION

This past year DOT made progress in establishing an effective information security program by issuing overdue information security policies. These policies will serve as the starting point to improve DOT's information security program. However, because most DOT systems are owned and managed by the Operating Administrations, ensuring proper implementation and execution of these security policies will require strong leadership, greater influence, and oversight by the DOT OCIO, and management commitment from Operating Administration Administrators to achieve a mature information security program that is sustainable. Until DOT addresses known weaknesses in its program, it will remain vulnerable to unauthorized and potentially malicious parties.

RECOMMENDATIONS

Recognizing the challenges to develop a mature information security program from what DOT has currently in place, we are providing a number of actions that 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. Revise the incident response policy to identify conditions under which incidents should be reported to law enforcement (i.e., OIG), how the reporting should be performed, what evidence should be collected, and how it should be collected.
2. 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.
3. 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.
4. 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.
5. 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.

6. 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.

Enterprise-Level Weaknesses:

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.
8. Use automated tools to periodically verify status of completion reported by Operating Administrations and identify deviations from the approved baseline configurations.
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.
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.
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.
12. Develop and establish a tracking system that effectively and routinely accounts for all active contractors requiring security awareness training.
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.
14. Identify and ensure all employees with significant security responsibilities take the necessary specialized security training to fulfill their responsibilities.

Management of Security Weaknesses:

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.
16. Ensure accurate information is used to monitor Operating Administrations' progress in correcting security weaknesses.

Information System Security:

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.
18. Ensure that Maritime Administration properly inventories its information systems and tracks them in the Cyber Security Assessment and Management system.
19. Ensure that Maritime Administration certifies and accredits each system in the revised inventory.
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.
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.
22. Develop a process to ensure Operating Administrations continuously monitor and test information system security controls.

Privacy Program:

23. Finalize the inventory count for systems containing privacy information.
24. Work with Operating Administrations to complete privacy impact assessments for applicable information systems.
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.
26. Implement 2-factor authentication for remote access.
27. Implement NIST-approved encryption on all mobile computers/devices.

MANAGEMENT COMMENTS

A draft of this report was provided to the Department's CIO on November 9, 2009. On November 16, 2009, we received the Department CIO's response, which can be found in its entirety in the Appendix. The CIO generally concurred with our findings and recommendations and will provide, in 30 days, written comments describing the specific actions and milestones that will be taken to implement the recommendations.

ACTIONS REQUIRED

We will review the Chief Information Officer's detailed action plans 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; Ann Calvaresi-Barr, Principal Assistant Inspector General for Auditing and Evaluation, at (202) 366-1427; or Rebecca C. Leng, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

cc: Deputy Secretary
Assistant Secretary for Budget and Programs/Chief Financial Officer
CIO Council Members
Martin Gertel, M-1

EXHIBIT A. Scope and Methodology

The Federal Information Security Management Act of 2002 (FISMA) requires 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 August 20, 2009, the Office of Management and Budget (OMB) issued M-09-29, FY 2009 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 2009, 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 45 departmental systems (see Table 8) 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. We also conducted testing to assess the Department's inventory, its overall process of resolving information security weaknesses, certain privacy requirements, configuration management, incident reporting, security-awareness training, and peer-to-peer file sharing. 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.

Table 8. OIG's Representative Subset of DOT Systems

Operating Administration	System	Impact Level	Contractor System?
FAA	Accident/Incident & Enforcement Query Tool (AIE)	Moderate	No
FAA	ASH HQ LAN	Moderate	No
FAA	ASH LANS	Moderate	No
FAA	ATO Consolidated LAN	Low	No
FAA	ATO Network	Moderate	No
FAA	Aviation Safety Information Analysis and Sharing (ASIAS) System	Moderate	No
FAA	Capability and Architecture Tool Suite (CATS-I)	Low	No
FAA	Collaborative Routing Coordination Tool (CRCT)	Low	No

Operating Administration	System	Impact Level	Contractor System?
FAA	Delphi Tracking System (DTF)	Moderate	No
FAA	Eastern Region Office of Government Ethics – 450 (OGE-450)	Moderate	No
FAA	Enterprise Architecture Portal (EAP) Metadata Repository	Low	No
FAA	Excellence through Quality Reliance (EtQ)	Moderate	No
FAA	Flight Service for the 21st Century (FS21)	Moderate	No
FAA	Flight Systems Laboratory Software Tool Set (FSL Tools)	Low	No
FAA	Information Technology Asset Management System (ITAMS)	Low	No
FAA	Integrated Rulemaking Management Information System (IRMIS)	High	No
FAA	Monitor Safety Related Data / Aviation Safety Accident Prevention Program (MSRD/ASAP)	Moderate	No
FAA	NADIN Message Switch Rehost (NMR)	Moderate	No
FAA	National Airspace System Technical Evaluation Program (NASTEP)	Low	No
FAA	Office of Airports Local Area Networks (ARP LANS)	Moderate	No
FAA	Operations Specifications Sub-System (OPSS)	High	No
FAA	Payback	Moderate	No
FAA	Risk Based Resource Targeting (RBRT)	Moderate	No
FAA	Safety Program Notification System (SPANS)	Moderate	No
FAA	Selections Within Faster Times (SWIFT)	Moderate	No
FAA	Staffing and Cost Analysis Tool (SCAT)	Moderate	No
FAA	Voice Switching and Control System (VSCS)	Moderate	No
FAA	Whistleblower Protection Program (WBPP)	High	No
FHWA	Delphi Interface Maintenance System (DIMS)	High	No
FMCSA	Commercial Vehicle Information Systems & Networks (CVISN) Web Site	Low	No
FMCSA	COMPASS	Moderate	No
FMCSA	Gotham	Moderate	No
FRA	Railroad Credit Risk Assessment	Low	No
FTA	FTA Inter/Intranet	Moderate	Yes

Exhibit A. Scope and Methodology

Operating Administration	System	Impact Level	Contractor System?
FTA	National Transit Database (NTD)	Moderate	Yes
MARAD	Enclave 1	Low	No
NHTSA	Support Delivery Services	Moderate	No
OST	Case Tracking System (CTS)	Moderate	No
OST	Correspondence Control Management System (CCMS)	Moderate	No
OST	Grant Information System (GIS)	Low	Yes
OST	Security Operations Systems	High	Yes
OST	Transportation Integrated Print Transaction System (TIPTS)	Low	Yes
OST	Workman Compensation Information System (WCIS)	Moderate	No
PHMSA	NPMS	Low	Yes
RITA	Volpe Center PRISM System	Moderate	Yes

Source: OIG

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

As required, we submitted to OMB key security metrics and 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. For 2009, OMB changed a number of security metrics and assessments, and mandated the use of the Web-based CyberScope system to input our FISMA results. In addition to preparing our submission, we reviewed the Department's progress in resolving weakness identified in our prior year's FISMA report.

We performed our information security review work between February 2009 and September 2009. 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.

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:

DOT Information Security Program, FI-2009-003, October 8, 2008;
DOT Information Security Program, FI-2008-001, October 10, 2007;
DOT Information Security Program, FI-2007-002, October 23, 2006;

Exhibit A. Scope and Methodology

DOT Information Security Program, FI-2006-002, October 7, 2005;
DOT Information Security Program, FI-2005-001, October 1, 2004;
DOT Information Security Program, FI-2003-086, September 25, 2003;
DOT Information Security Program, FI-2002-115, September 27, 2002; and
DOT Information Security Program, FI-2001-090, September 7, 2001.

Exhibit A. Scope and Methodology

EXHIBIT B. DOT OPERATING ADMINISTRATIONS AND SYSTEM INVENTORY COUNTS

Operating Administration	FY 2009	FY 2008
Federal Aviation Administration (FAA)	274	264
Federal Highway Administration (FHWA)	21	26
Federal Motor Carrier Safety Administration (FMCSA)	21	23
Federal Railroad Administration (FRA)	12	21
Federal Transit Administration (FTA)	5	5
Maritime Administration (MARAD)	10	13
National Highway Traffic Safety Administration (NHTSA)	10	11
Office of Inspector General (OIG)	2	2
Office of the Secretary (OST)	36	44
Pipeline and Hazardous Materials Safety Administration (PHMSA)	5	4
Research and Innovative Technology Administration (RITA)	10	9
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1
Surface Transportation Board (STB)	2	2
Total Systems	409	425

Source: OIG, and DOT CSAM as of July 6, 2009

Exhibit B. DOT Operating Administrations and System Inventory Counts

EXHIBIT C. Status of Prior Year's Recommendations

FY 2008 FISMA Report Recommendation Number	FY 2008 Recommendation	Status
1	Provide information security performance metrics to be included in Operating Administration CIOs' performance standards and subsequently provide input on their performance in addressing these metrics.	CLOSED
2	Develop and issue comprehensive, compliant information security policies and procedures as required by FISMA, OMB, and NIST.	CLOSED
3	Complete review of its draft breach-notification policy, perform revisions as necessary to conform to OMB requirements, and issue an official breach-notification policy.	CLOSED
4	Review and finalize its plan to reduce Social Security numbers, and implement the reduction of Social Security numbers in the time frame set forth by OMB.	OPEN
5	Issue a policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to protect privacy.	CLOSED
6	Establish a departmentwide internal FISMA cut-off date that allows sufficient time for the Department to conduct meaningful internal review, which includes evaluating the accuracy of the data it includes in its FISMA report as well as time to resolve any potential disputes with the OIG.	CLOSED
7	Maintain an adequate audit trail of data supporting FISMA reports as of the selected cut-off date.	CLOSED
8	Assign a priority to finalizing the DOT configuration management policy.	CLOSED

FY 2008 FISMA Report Recommendation Number	FY 2008 Recommendation	Status
9	Require Operating Administrations to periodically report status of baseline configuration compliance and independently validate compliance status reported by Operating Administrations.	CLOSED
10	Implement NIST Federal Desktop Core Configuration settings on the Window XP workstations on the DOT Common Operating Environment, require Operating Administrations to implement Federal Desktop Core Configuration settings on Operating Administrations' Windows XP workstations, and document any required deviations from those settings.	CLOSED
11	Establish a timetable for Operating Administrations to work with CSMC to deploy monitoring devices covering all DOT critical networks	CLOSED
12	Enforce Operating Administrations' reporting of PII-related security incidents to CSMC immediately upon discovery, as specified in DOT policy.	CLOSED
13	Revised DOT policies to meet the OMB requirement for reporting PII incidents.	CLOSED
14	Implement procedures for Operating Administrations to take timely remedial action for identified incidents.	CLOSED
15	Direct CSMC and Operating Administrations to work together to collect and share the information needed for cyber incident-response reporting, such as IP-address assignment and critical logging data.	CLOSED
16	Enforce the requirements for all employees and contractors to take security-awareness training in order to gain and maintain access to Department systems.	CLOSED*
17	Establish a tracking system or other process that effectively and routinely accounts for all active contractors requiring security training.	CLOSED*

Exhibit C. Status of Prior Year's Recommendations

FY 2008 FISMA Report Recommendation Number	FY 2008 Recommendation	Status
18	Establish a mechanism to identify and train employees and contractors requiring specialized security training.	CLOSED*
19	Include collaborative Web technologies in the Department's required security-awareness training.	OPEN
20	Ensure that all weaknesses that are identified during reviews, including certification and accreditation, and that require remediation, are tracked in the Department's POA&M system.	CLOSED*
21	Establish adequate policies for timeliness of remediation and enforce such policies.	CLOSED
22	Require that all identified weaknesses include a cost estimate and that these estimates, along with the severity of the weakness, be used to prioritize these weaknesses for correction.	CLOSED
23	Implement a process to ensure that all departmental systems that require e-authentication are identified in the e-authentication system inventory and that the necessary e-authentication supporting documentation is obtained or developed for these systems.	CLOSED
24	Ensure that all systems that require e-authentication have certification and accreditation packages that include support for e-authentication in the appropriate sections of their system security plans and risk assessments.	CLOSED
25	Validate that e-authentication systems have operationally achieved the required assurance level.	OPEN
26	Require development and appropriate annual testing of system contingency plans and ensure that tested contingency plans are updated based on the results of the contingency plan tests performed, and	CLOSED*
27	Enforce certification and accreditation requirements uniformly throughout the Department.	CLOSED

Source: OIG

*New recommendations were made in this year's audit to continue addressing these deficiencies.

Exhibit C. Status of Prior Year's Recommendations

EXHIBIT D. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis C. King	Program Director
Dr. Ping Z. Sun	Program Director for IT Audit Computer Laboratory
Michael Marshlick	Project Manager
Lissette Mercado	Project Manager
Karen Sloan	Communications Officer
Atul Darooka	Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Ann Moles	Information Technology Specialist
Anthony Cincotta	Information Technology Specialist
Vasily Gerasimov	Information Technology Specialist

APPENDIX. MANAGEMENT COMMENTS

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

1200 New Jersey Ave., S.E.
Washington, DC 20590

November 16, 2009

To: Calvin L. Scovel, III
DOT Inspector General

From: Nitin Pradhan
DOT Chief Information Officer

Prepared By: Andrew R. Orndorff
DOT Chief Information Security Officer

Subject: Chief Information Officer's Response to Inspector General's FISMA 2009 Assessment Report, FI–2010–XXX, "AUDIT OF DOT's INFORMATION SECURITY PROGRAM AND PRACTICES"

The Department of Transportation (DOT) Chief Information Officer (CIO) reviewed and assessed the Office Of Inspector General's (OIG's) draft final FY 2009 Information Security Program Audit Report (Report Number: FI-2010-XXX) and the DOT CIO generally concurs with the report's findings, and will provide a corrective action plan to address the recommendations 30 days after the signing date of the official FY 2009 FISMA report.

The DOT CIO believes that an enhanced, holistic business strategy is required to rapidly strengthen the department's ability to ensure the confidentiality, integrity, and availability of its vital data and assets. While the approach leveraged in previous years resulted in incremental improvements to the departmental privacy and cyber security posture, minimal progress was made in addressing root causes relating to people, processes, and technology. In the interim, risks to departmental systems and data have increased with the introduction of new business requirements, new technologies, and as cyber attackers have become more sophisticated, these risks are outpacing DOT efforts and resources. In response, the CIO is preparing an action plan that focuses on people, process, and technology, and that will apply an iterative approach by first identifying the most serious risks and targeting the most critical vulnerabilities. Policy, plans, and process will be established to improve the security posture and to mitigate the risk. This process will be repeated for each risk area and vulnerability. The target goals are rapid improvements to DOT cyber security and privacy, and will establish repeatable and measurable processes. The CIO also plans to enforce linkage between cyber security and privacy investments, and the departmental capital planning process, to monitor performance, ensure accountabilities, and to make decisions on investment priorities and resources. It should be noted, however, that execution of this plan may require organizational or operational changes, multiple years of effort, and additional funding and resources.

The CIO has already started taking action to reinforce the overarching security posture of the department, including, but not limited to the following:

- The CIO has established a departmental Cyber Security and Privacy council and is developing a cyber security and privacy plan, with a balance of strategic, operational, tactical and innovative solutions aligned with Federal and agency mission goals, and incorporating lessons learned from other agencies and the private sector.

- The CIO is upgrading cyber security management systems, will work with the operating administrations to improve data quality and accuracy in reporting of weaknesses, and will evaluate and implement a dashboard, with sustainable metrics, to accurately monitor and report on DOT performance.

- The CIO is working to engage Federal agencies to perform a vulnerability assessment to identify the most critical vulnerabilities of DOT networks and systems, and is updating the DOT system inventory to identify the most critical DOT assets and systems. The resulting information will be used to guide corrective actions and investments in order to mitigate the most serious risks.

- The CIO is partnering with leading Federal agencies and the private sector to acquire tools that, when deployed, will strengthen security awareness, enhancing the knowledge of DOT personnel. Additionally, the CIO is evaluating partnering with Federal agencies, academia, and the private sector to develop and provide innovative security training appropriate for personnel with security responsibilities.

- The CIO will exploit opportunities to leverage the capabilities of technologies which DOT already owns, such as desktop and server technologies licensed from Microsoft, to strengthen the security of DOT common information technology infrastructure, and to gain early and important cyber security and privacy improvements at the lowest possible incremental investment.

- The CIO is incorporating enhancements to the DOT cyber security and privacy program into the plans, which will address current gaps and ensure that safeguards to protect the confidentiality, integrity and availability of DOT systems and data are integrated into and support the mission of DOT. These enhancements include implementing the National Institute of Standards and Technology (NIST) risk management framework and shifting to continuous monitoring for DOT systems and services.

Lastly, the CIO has directed the DOT Chief Information Security Officer (CISO) to meet at least monthly with the OIG as a means to improve information sharing, ensure understanding of requirements and metrics that the CIO is utilizing, and report upon progress and issues affecting the program throughout the FISMA performance year.

If you have any questions, please feel free to call me at 202-366-9201 or have a member of your staff call Andrew Orndorff on 202-366-7111.

cc: Rebecca Leng, JA-20
Martin Gertel, M-1

Appendix. Management Comments

Year 2009 Audit of Department of Transportation's Information Security Program and Practice Report

Section 508 Compliant Presentation

Table 1 depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report on page 5 titled "Examples of Information Security Policy Deficiencies by Program Area."

This table presents the Department of Transportation's policies that lacked critical elements to effectively and adequately guide the agency's information security program or address key Office of Management and Budget privacy requirements.

The following presents the status of Information Security Policy Deficiencies by Program Area.

Functional Description, Program Area, Incident Reporting, defined as detecting, reporting, and responding to security incidents, including notifying law enforcement agencies and relevant Offices of Inspector General. Office of Inspector General Policy Evaluation**,** the policy does not document the requirement to report incidents to law enforcement and the Office of Inspector General as required by the Federal Information Security Management Act and the Office of Management and Budget.

Functional Description, Program Area, Plans of Action and Milestones, used to track the measures implemented to correct deficiencies and to reduce or eliminate known vulnerabilities. Office of Inspector General Policy Evaluation, the policy does not specifically identify the required data elements to properly document and report on information systems' or programs' security weaknesses throughout the lifecycle as required by the Office of Management and Budget. Such information includes: Description of Weaknesses, Scheduled Completion Date, Key Milestones with Completion Dates, Milestone Changes, Source (for example, program review, IG audit, GAO audit, etcetera.), and Status.

Functional Description, Program Area, Security Training, defined as disseminating security information that the workforce, both employees and contractors, need to do their job. OIG Policy Evaluation, the policy did not address the identification of users with login privileges to the Department information systems. In addition, it does not identify specific job functions that require specialized security training, such as Chief Information Officer, Information System Security Officer, Database Administrator, etcetera.

Functional Description, Program Area, Contractor Oversight, defined as monitoring the effectiveness of the information security for information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Office of Inspector General Policy Evaluation, the policy did not contain contractor oversight provisions that would ensure that proper security for the contracted information and systems are in adherence with National Institute of Standards and Technology, Office of Management and Budget, and Federal Information Security Management Act requirements.

Functional Description, Program Area, External Interfaces, defined as enforcing System Interconnection/Information Sharing and Interconnection Security Agreement, Memorandum of Understanding, or Memorandum of Agreement between systems that share data that are owned or operated by different organizations. Office of Inspector General Policy Evaluation, the policy does not provide any guidance on the preparation of these critical interface agreements nor does it address key elements of National Institute of Standards and Technology guidance.

Table 2 depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report on page 7 titled "Summary of Incidents Missing United States Computer Emergency Readiness Team Reference Numbers."

This table presents the number of security incidents which did not have a United States Computer Emergency Readiness Team reference numbers for each incident category type.

Incidents Missing Reference Numbers, Category 1, Unauthorized Access (for example, Personally Identifiable Information Breach), 107, Percentage, 14.

Incidents Missing Reference Numbers, Category 2, Denial of Service, 0, Percentage, 0.

Incidents Missing Reference Numbers, Category 3, Malicious Code, 393, Percentage, 53.

Incidents Missing Reference Numbers, Category 4, Improper Usage, 170, Percentage, 23.

Incidents Missing Reference Numbers, Category 5, Scans, Probes, Attempted Access, 73, Percentage, 10.

Incidents Missing Reference Numbers, Total Security Incidents, 743, Percentage 100.

Table 3, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, on page 9, titled "Unreported Job Functions and Estimated Employees Requiring Specialized Training."

This table presents the number of estimated employees, grouped by job function and Operating Administration, that should have taken specialized training, but did not.

Chief Information Officer, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of Inspector General, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 9.

Information System Security Officer or Information System Security Manager, Federal Transit Administration, 1, Office of the Secretary, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 4.

System Administrator, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 8.

System Designer and Developers, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of Inspector General, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 9.

Network Administrator, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 8.

Database Administrator, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of Inspector General, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 9.

System Certifier, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office

of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 8.

Designated Authorizing Authority, Federal Railroad Administration, 1, Federal Transit Administration, 1, Maritime Administration, 1, National Highway Traffic Safety Administration, 1, Office of the Secretary, 1, Research and Innovative Technology Administration, 1, Saint Lawrence Seaway Development Corporation, 1, Surface Transportation Board, 1, Total Unreported, 8.

Total Unreported, Federal Railroad Administration, 7, Federal Transit Administration, 8, Maritime Administration, 7, National Highway Traffic Safety Administration, 7, Office of Inspector General, 3, Office of the Secretary, 8, Research and Innovative Technology Administration, 7, Saint Lawrence Seaway Development Corporation, 8, Surface Transportation Board, 8, Total Unreported, 63.

Table 4, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, on page 10, titled "Summary of Overdue Plan of Action and Milestones."

This table presents the number of Open Plan of Action and Milestones for each Operating Administration and a breakdown how long overdue they are, how many did not have target completion dates, and how many had future scheduled completion dates.

DOT Programs, Total Plan of Action of Milestones, 69, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 1, more than a year overdue, 64, Total Overdue, 65, No Target Completion Date, 1, Future Scheduled Completion Date, 3.

Federal Aviation Administration, Total Plan of Action of Milestones, 4397, 1 to 60 days overdue, 148, 61 to 90 days overdue, 34, 91 to 120 days overdue, 14, 121 to 1 year overdue, 56, more than a year overdue, 9, Total Overdue, 261, No Target Completion Date, 7, Future Scheduled Completion Date, 4129.

Federal Highway Administration, Total Plan of Action of Milestones, 514, 1 to 60 days overdue, 52, 61 to 90 days overdue, 0, 91 to 120 days overdue, 1, 121 to 1 year overdue, 73, more than a year overdue, 89, Total Overdue, 215, No Target Completion Date, 0, Future Scheduled Completion Date, 299.

Federal Motor Carrier Safety Administration, Total Plan of Action of Milestones, 3, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 2, Total Overdue, 2, No Target Completion Date, 0, Future Scheduled Completion Date, 1.

Federal Railroad Administration, Total Plan of Action of Milestones, 20, 1 to 60 days overdue, 20, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 0, Total Overdue, 20, No Target Completion Date, 0, Future Scheduled Completion Date, 0.

Federal Transit Administration, Total Plan of Action of Milestones, 50, 1 to 60 days overdue, 5, 61 to 90 days overdue, 7, 91 to 120 days overdue, 0, 121 to 1 year overdue, 23, more than a year overdue, 0, Total Overdue, 35, No Target Completion Date, 0, Future Scheduled Completion Date, 15.

Maritime Administration, Total Plan of Action of Milestones, 0, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 0, Total Overdue, 0, No Target Completion Date, 0, Future Scheduled Completion Date, 0.

National Highway Traffic Safety Administration, Total Plan of Action of Milestones, 7, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 6, Total Overdue, 6, No Target Completion Date, 0, Future Scheduled Completion Date, 1.

Office of Inspector General, Total Plan of Action of Milestones, 18, 1 to 60 days overdue, 2, 61 to 90 days overdue, 2, 91 to 120 days overdue, 2, 121 to 1 year overdue, 8, more than a year overdue, 0, Total Overdue, 14, No Target Completion Date, 2, Future Scheduled Completion Date, 2.

Office of the Secretary, Total Plan of Action of Milestones, 149, 1 to 60 days overdue, 10, 61 to 90 days overdue, 0, 91 to 120 days overdue, 127, 121 to 1 year overdue, 0, more than a year overdue, 0, Total Overdue, 137, No Target Completion Date, 1, Future Scheduled Completion Date, 11.

Pipeline and Hazardous Materials Safety Administration, Total Plan of Action of Milestones, 128, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 128, Total Overdue, 128, No Target Completion Date, 0, Future Scheduled Completion Date, 0.

Research and Innovative Technology Administration, Total Plan of Action of Milestones, 19, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 1, Total Overdue, 1, No Target Completion Date, 18, Future Scheduled Completion Date, 0.

Saint Lawrence Seaway Development Corporation, Total Plan of Action of Milestones, 1, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1

year overdue, 0, more than a year overdue, 0, Total Overdue, 0, No Target Completion Date, 1, Future Scheduled Completion Date, 0.

Surface Transportation Board, Total Plan of Action of Milestones, 67, 1 to 60 days overdue, 0, 61 to 90 days overdue, 0, 91 to 120 days overdue, 0, 121 to 1 year overdue, 0, more than a year overdue, 52, Total Overdue, 52, No Target Completion Date, 15, Future Scheduled Completion Date, 0.

Total, Total Plan of Action of Milestones, 5442, 1 to 60 days overdue, 237, Percentage, 4, 61 to 90 days overdue, 43, Percentage, 1, 91 to 120 days overdue, 144, Percentage, 3, 121 to 1 year overdue, 161, Percentage, 3, more than a year overdue, 351, Percentage, 6, Total Overdue, 936, Percentage, 17, No Target Completion Date, 45, Percentage, 1, Future Scheduled Completion Date, 4461, Percentage, 82.

Table 5, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, on page 11, titled "OIG Plan of Action and Milestone Data Analysis Comparison Results."

This table presents the discrepancies found between the Plan of Action and Milestone database and the Security and Privacy Posture Summary Status Report, which is used by the Office of the Chief Information Officer to monitor Operating Administrations' progress in correcting identified security weaknesses.

Total Number of Open Plan of Action Milestones, Office of the Chief Information Officers Report, 4674, Plan of Action and Milestones Database, 5442, Difference, 768.

Plan of Action and Milestones not Categorized, Office of the Chief Information Officers Report, 247, Plan of Action and Milestones Database, 395, Difference, 148.

Unidentified Cost, Office of the Chief Information Officers Report, 0, Plan of Action and Milestones Database, 2393, Difference, 2393.

Overdue Plan of Action of Milestones, Office of the Chief Information Officers Report, 276, Plan of Action and Milestones Databse, 936, Difference, 660.

Table 6, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, on page 14, titled "Sample Systems Results Summary by Operating Administration."

This table summarizes our review of the sampled certification and accreditation packages provided by Operating Administrations. The table provides the number of systems sampled in each Operating Administration, the number of systems with non-compliant

certification and accreditations, the number of systems without annual testing, and the number of systems without tested contingency plans.

Number of Sampled Systems, Federal Aviation Administration, 28, Federal Highway Administration, 1, Federal Motor Carrier Safety Administration, 3, Federal Railroad Administration, 1, Federal Transit Administration, 2, Maritime Administration, 1, National Highway Transportation Safety Administration, 1, Office of the Secretary, 6, Pipeline and Hazardous Materials Safety Administration, 1, Research and Innovative Technology Administration, 1, Total 45.

Systems without fully compliant certification and accreditations, Federal Aviation Administration, 22, Federal Highway Administration, 0, Federal Motor Carrier Safety Administration, 0, Federal Railroad Administration, 0, Federal Transit Administration, 0, Maritime Administration, 1, National Highway Transportation Safety Administration, 0, Office of the Secretary, 2, Pipeline and Hazardous Materials Safety Administration, 0, Research and Innovative Technology Administration, 0, Total 25.

Systems without annual testing, Federal Aviation Administration, 5, Federal Highway Administration, 0, Federal Motor Carrier Safety Administration, 2, Federal Railroad Administration, 0, Federal Transit Administration, 0, Maritime Administration, 1, National Highway Transportation Safety Administration, 1, Office of the Secretary, 0, Pipeline and Hazardous Materials Safety Administration, 0, Research and Innovative Technology Administration, 0, Total 9.

Systems without tested contingency plans, Federal Aviation Administration, 16, Federal Highway Administration, 1, Federal Motor Carrier Safety Administration, 0, Federal Railroad Administration, 1, Federal Transit Administration, 0, Maritime Administration, 1, National Highway Transportation Safety Administration, 0, Office of the Secretary, 2, Pipeline and Hazardous Materials Safety Administration, 1, Research and Innovative Technology Administration, 0, Total 22.

Table 7, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, on page 15, titled "DOT Implementation of Office of Management and Budget Privacy Initiatives."

This table summarizes the Department of Transportation's status in implementing the Office of Management and Budget privacy initiatives in the areas of social security number reduction, two-factor authentication, and encryption of personally identifiable information on mobile devices.

OMB Initiative, Complete Social Security Number and Personally Identifiable Information Reduction, Status, the Department of Transportation identified 25 systems

that can reduce use of social security numbers. Only 5 systems have completed a plan to do so. In addition, FAA does not plan to eliminate unnecessary use of social security numbers until 2015.

OMB Initiative, Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access, Status, Two-factor authentication delayed until the Department of Transportation implements Homeland Security Presidential Directive 12.

OMB Initiative, ensure that all personally identifiable information stored or carried on mobile computers and devices is encrypted using National Institute of Standards and Technology approved encryption. Status, as of July 2, 2009, 592 out of 11723 mobile devices from the Department have not had National Institute of Standards and Technology approved encryption applied. However, no data were available for Federal Aviation Administration and Federal Highway Administration.

Table 8, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report on page 20, 21, 22 and 23, titled "Office of Inspector General's Representative Subset of Department of Transportation Systems."

This table lists the 45 systems selected as part of the Office of Inspector General's representative sample of the Department of Transportation's systems along with their corresponding Operating Administration, Impact Level, and whether it is a contractor system.

Operating Administration, Federal Aviation Administration, System Name, Accident/Incident and Enforcement Query Tool, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Security and Hazardous Materials Office Headquarter Local Area Network, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Security and Hazardous Materials Office Local Area Networks, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Air Traffic Organization Consolidated Local Area Network, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Air Traffic Organization Network, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Aviation Safety Information Analysis and Sharing System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Capability and Architecture Tool Suite, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Collaborative Routing Coordination Tool, Impact Level, Low, Contractor System, No.
Operating Administration, Federal Aviation Administration, System Name, Delphi Tracking System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Eastern Region Office of Government Ethics 450, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Enterprise Architecture Portal Metadata Repository, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Excellence through Quality Reliance, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Flight Service for the Twenty First Century, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Flight Systems Laboratory Software Tool Set, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Information Technology Asset Management System, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Integrated Rulemaking Management Information System, Impact Level, High, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Monitor Safety Related Data / Aviation Safety Accident Prevention Program, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, National Airspace Data Interchange Network Message Switch Rehost, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, National Airspace System Technical Evaluation Program, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Office of Airports Local Area Networks, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Operations Specifications Sub-System, Impact Level, High, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Payback, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Risk Based Resource Targeting, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Safety Program Notification System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Selections Within Faster Times, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Staffing and Cost Analysis Tool, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Voice Switching and Control System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Aviation Administration, System Name, Whistleblower Protection Program, Impact Level, High, Contractor System, No.

Operating Administration, Federal Highway Administration, System Name, Delphi Interface Maintenance System, Impact Level, High, Contractor System, No.

Operating Administration, Federal Motor Carrier Safety Administration, System Name, Commercial Vehicle Information Systems and Networks Web Site, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Motor Carrier Safety Administration, System Name, Compass, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Motor Carrier Safety Administration, System Name, Gotham, Impact Level, Moderate, Contractor System, No.

Operating Administration, Federal Railroad Administration, System Name, Railroad Credit Risk Assessment, Impact Level, Low, Contractor System, No.

Operating Administration, Federal Transit Administration, System Name, Federal Transit Administration Internet Intranet, Impact Level, Moderate, Contractor System, Yes.

Operating Administration, Federal Transit Administration, System Name, National Transit Database, Impact Level, Moderate, Contractor System, Yes.

Operating Administration, Maritime Administration, System Name, Enclave 1, Impact Level, Low, Contractor System, No.

Operating Administration, National Highway Transportation Safety Administration, System Name, Support Delivery Services, Impact Level, Moderate, Contractor System, No.

Operating Administration, Office of the Secretary, System Name, Case Tracking System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Office of the Secretary, System Name, Correspondence Control Management System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Office of the Secretary, System Name, Grant Information System, Impact Level, Low, Contractor System, Yes.

Operating Administration, Office of the Secretary, System Name, Security Operations Systems, Impact Level, High, Contractor System, Yes.

Operating Administration, Office of the Secretary, System Name, Transportation Integrated Print Transaction System, Impact Level, Low, Contractor System, Yes.

Operating Administration, Office of the Secretary, System Name, Workman Compensation Information System, Impact Level, Moderate, Contractor System, No.

Operating Administration, Pipeline and Hazardous Materials Safety Administration, System Name, National Pipeline Management System, Impact Level, Low, Contractor System, Yes.

Operating Administration, Research and Innovative Technology Administration, System Name, Volpe Center PRISM System, Impact Level, Moderate, Contractor System, Yes.

Exhibit B, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report, page 24, titled "Department of Transportation Operating Administrations and System Inventory Counts." This table provides the number of systems reported by each Operating Administration in Fiscal Years 2008 and 2009.

Federal Aviation Administration reported 274 systems in Fiscal Year 2009 and 264 systems in Fiscal Year 2008.

Federal Highway Administration reported 21 systems in Fiscal Year 2009 and 26 systems in Fiscal Year 2008.

Federal Motor Carrier Safety Administration reported 21 systems in Fiscal Year 2009 and 23 systems in Fiscal Year 2008.

Federal Railroad Administration reported 12 systems in Fiscal Year 2009 and 21 systems in Fiscal Year 2008.

Federal Transit Administration reported 5 systems in Fiscal Year 2009 and 5 systems in Fiscal Year 2008.

Maritime Administration reported 10 systems in Fiscal Year 2009 and 13 systems in Fiscal Year 2008.

National Highway Traffic Safety Administration reported 10 systems in Fiscal Year 2009 and 11 systems in Fiscal Year 2008.

Office of Inspector General reported 2 systems in Fiscal Year 2009 and 2 systems in Fiscal Year 2008.

Office of the Secretary reported 36 systems in Fiscal Year 2009 and 44 systems in Fiscal Year 2008.

Pipeline and Hazardous Materials Safety Administration reported 5 systems in Fiscal Year 2009 and 4 systems in Fiscal Year 2008.

Research and Innovative Technology Administration reported 10 systems in Fiscal Year 2009 and 9 systems in Fiscal Year 2008.

Saint Lawrence Seaway Development Corporation reported 1 system in Fiscal Year 2009 and 1 system in Fiscal Year 2008.

Surface Transportation Board reported 2 systems in Fiscal Year 2009 and 2 systems in Fiscal Year 2008.

In total, the Department of Transportation reported 409 systems in Fiscal Year 2009 and 425 systems in Fiscal Year 2008.

Exhibit C, depicted in the Fiscal Year 2009 Audit of Department of Transportation's Information Security Program and Practices Report on pages 25, 26, and 27, titled "Status of Prior Year's Recommendations." This table provides a listing of the recommendations made in the Fiscal Year 2008 Federal Information Security Management Act audit and their current status.

Fiscal Year 2008, Recommendation 1, Provide information security performance metrics to be included in Operating Administration Chief Information Officers performance standards and subsequently provide input on their performance in addressing these metrics, Status, Closed.

Fiscal Year 2008, Recommendation 2, Develop and issue comprehensive, compliant information security policies and procedures as required by the Federal Information Security Management Act, the Office of Management and Budget, and the National Institute of Standards and Technology, Status, Closed.

Fiscal Year 2008, Recommendation 3, Complete review of its draft breach-notification policy, perform revisions as necessary to conform to the Office of Management and Budget requirements, and issue an official breach-notification policy, Status, Closed.

Fiscal Year 2008, Recommendation 4, Review and finalize its plan to reduce Social Security numbers, and implement the reduction of Social Security numbers in the time frame set forth by Office of Management and Budget, Status, Open.

Fiscal Year 2008, Recommendation 5, Issue a policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to protect privacy, Status, Closed.

Fiscal Year 2008, Recommendation 6, Establish a department-wide internal Federal Information Security Management Act cut-off date that allows sufficient time for the Department to conduct meaningful internal review, which includes evaluating the accuracy of the data it includes in its Federal Information Security Management Act

report as well as time to resolve any potential disputes with the Office of the Inspector General, Status, Closed.

Fiscal Year 2008, Recommendation 7, Maintain an adequate audit trail of data supporting the Federal Information Security Management Act reports as of the selected cut-off date, Status, Closed.

Fiscal Year 2008, Recommendation 8, Assign a priority to finalizing the Department of Transportation configuration management policy, Status, Closed.

Fiscal Year 2008, Recommendation 9, Require Operating Administrations to periodically report status of baseline configuration compliance and independently validate compliance status reported by Operating Administrations, Status, Closed.

Fiscal Year 2008, Recommendation 10, Implement National Institute of Standards and Technology Federal Desktop Core Configuration settings on the Window X.P. workstations on the Department of Transportation Common Operating Environment, require Operating Administrations to implement Federal Desktop Core Configuration settings on Operating Administrations Windows X.P. workstations, and document any required deviations from those settings, Status, Closed.

Fiscal Year 2008, Recommendation 11, Establish a timetable for Operating Administrations to work with the Cyber Security Management Center to deploy monitoring devices covering all Department of Transportation critical networks, Status, Closed.

Fiscal Year 2008, Recommendation 12, Enforce Operating Administrations' reporting of Personally Identifiable Information related security incidents to the Cyber Security Management Center immediately upon discovery, as specified by Department of Transportation policy, Status, Closed.

Fiscal Year 2008, Recommendation 13, Revise Department of Transportation policies to meet the Office of Management and Budget requirement for reporting Personally Identifiable Information incidents, Status, Closed.

Fiscal Year 2008, Recommendation 14, Implement procedures for Operating Administrations to take timely remedial action for identified incidents, Status, Closed.

Fiscal Year 2008, Recommendation 15, Direct the Cyber Security Management Center and Operating Administrations to work together to collect and share the information needed for cyber incident-response reporting, such as I.P.-address assignment and critical logging data, Status, Closed.

Fiscal Year 2008, Recommendation 16, Enforce the requirements for all employees and contractors to take security-awareness training in order to gain and maintain access to Department systems, Status, Closed, however new recommendations were made in this year's audit to continue addressing these deficiencies.

Fiscal Year 2008, Recommendation 17, Establish a tracking system or other process that effectively and routinely accounts for all active contractors requiring security training, Status, Closed, however new recommendations were made in this year's audit to continue addressing these deficiencies.

Fiscal Year 2008, Recommendation 18, Establish a mechanism to identify and train employees and contractors requiring specialized security training, Status, Closed, however new recommendations were made in this year's audit to continue addressing these deficiencies.

Fiscal Year 2008, Recommendation 19, Include collaborative Web technologies in the Department's required security-awareness training, Status, Open.

Fiscal Year 2008, Recommendation 20, Ensure that all weaknesses that are identified during reviews, including certification and accreditation, and that require remediation, are tracked in the Department's POA&M system, Status, Closed, however new recommendations were made in this year's audit to continue addressing these deficiencies.

Fiscal Year 2008, Recommendation 21, Establish adequate policies for timeliness of remediation and enforce such policies, Status, Closed.

Fiscal Year 2008, Recommendation 22, Require that all identified weaknesses include a cost estimate and that these estimates, along with the severity of the weakness, be used to prioritize these weaknesses for correction, Status, Closed.

Fiscal Year 2008, Recommendation 23, Implement a process to ensure that all departmental systems that require e-authentication are identified in the e-authentication system inventory and that the necessary e-authentication supporting documentation is obtained or developed for these systems, Status, Closed.

Fiscal Year 2008, Recommendation 24, Ensure that all systems that require e-authentication have certification and accreditation packages that include support for e-authentication in the appropriate sections of their system security plans and risk assessments, Status, Closed.

Fiscal Year 2008, Recommendation 25, Validate that e-authentication systems have operationally achieved the required assurance level, Status, Open.

Fiscal Year 2008, Recommendation 26, Require development and appropriate annual testing of system contingency plans and ensure that tested contingency plans are updated based on the results of the contingency plan tests performed, Status, Closed, however new recommendations were made in this year's audit to continue addressing these deficiencies.

Fiscal Year 2008, Recommendation 27, Enforce certification and accreditation requirements uniformly throughout the Department, Status, Closed.