Office of Inspector General

Audit Report

FISMA 2016: DOT CONTINUES TO MAKE PROGRESS, BUT THE DEPARTMENT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE

Department of Transportation

Report Number: FI-2017-008
Date Issued: November 09, 2016

Memorandum

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

Subject: **ACTION:** FISMA 2016: DOT Continues To Make Progress, but the Department's Information Security Posture Is Still Not Effective
Department of Transportation
Report Number: FI-2017-008

Date: November 09, 2016

From: Calvin L. Scovel III
Inspector General

Reply to Attn. of: JA-20

To: Deputy Secretary

The Department of Transportation's (DOT) operations rely on 457 information technology (IT) systems, 317 (69 percent) of which belong to the Federal Aviation Administration (FAA). These systems represent an annual investment of approximately $3.5 billion—one of the largest IT investments among Federal civilian agencies. Moreover, the Department's financial IT systems are used to award, disburse, and manage approximately $99 billion in Federal funds annually.

An effective information security program—one that quickly identifies and addresses vulnerabilities—helps ensure continuity of agency operations and reduces the risk that individuals can gain unauthorized access to Federal systems and information. For DOT, secure information helps protect both taxpayers' dollars and citizens' safety since many of its systems control transportation-related operations including air traffic control and pilot licensing, while others support inspection and oversight of highway safety and transportation of hazardous materials.

The Federal Information Security Management Act of 2002 (FISMA),[1] as amended,[2] requires agencies to develop, implement, and document departmentwide information security programs. FISMA also requires chief

[1] Public Law No. 107-347 (2002).
[2] The Federal Information Security Modernization Act of 2014 (Public Law No. 113-283) amends FISMA to, among other things: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) for agency information security policies and practices; and (2) set authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of policies and practices for information systems.

information officers (CIO), inspectors general, and program officials to conduct annual reviews of their agencies' information security programs and report the results of these reviews to the Office of Management and Budget (OMB). For this fiscal year's review, OMB has required inspectors general to assess 166 metrics in five security function areas to determine information security program maturity[3] at one of five levels defined by OMB (from lowest to highest): Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, or Optimized.[4] OMB further defines effectiveness as meeting all metrics in the first four levels.

Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices for the 12-month period between July 1, 2015, and June 30, 2016.[5] Specifically, we assessed DOT's performance in the five function areas: (1) Identify; (2) Protect; (3) Detect; (4) Respond; and (5) Recover.[6]

We conducted our work in accordance with generally accepted Government auditing standards. To address OMB's 2016 FISMA reporting metrics, we tested a statistical sample of 75 out of 456 systems in the cybersecurity assessment and management system (CSAM) repository the Department uses to track system inventories, weaknesses, and other security information. The results of our statistical sample allowed us to estimate the percentage and number of systems complying with NIST and DHS requirements in the following areas: risk categorization; security plans; annual control testing; contingency planning; security authorization and continuous monitoring; incident handling; and plans of actions and milestones. See exhibit A for more details on our scope and methodology. As required, we provided our results to OMB via its Web portal.[7]

RESULTS IN BRIEF

Although the Department continues to make progress in implementing cybersecurity initiatives, its cybersecurity program remains ineffective based on OMB's methodology, which requires agencies to achieve a maturity level of Managed and Measurable to be considered effective. In the five function areas, DOT achieved maturity at the levels of Ad Hoc and Defined. In addition, the

[3] OMB's *FY 2016 Inspector General FISMA Act of 2014 Reporting Metrics* (September 2016) prescribes the metrics and provides a new methodology to assess the maturity of a program's function area.
[4] Table 1 in the Background explains the five functions and scoring criteria.
[5] Per OMB's *Annual Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, agencies should set cut-off dates for data collection and report preparation that allow adequate time for meaningful internal reviews, comments, and resolution of disputes before reports' finalization.
[6] OMB's function areas align to the National Institutes of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (2014).
[7] Because OMB designates this information "For Official Use Only," our submission to OMB is not contained in this report.

Department's information systems remain vulnerable to serious security threats due to the deficiencies in the five function areas discussed below:

1. **Identify.** DOT's Identify controls, which include security authorization, risk management and monitoring of weaknesses, among other things, are insufficient. The Department does not have a comprehensive risk management program. For example, seven Operating Administrations (OA) have allowed 70 systems' authorizations to operate expire. We also found that (1) seven OAs had deficiencies in the security control testing used to support system authorization; (2) the Office of the Chief Information Officer (OCIO) and the OAs have not established effective procedures for common security controls; (3) FAA and other OAs do not always manage their contractor operated systems according to requirements; and (4) OCIO does not sufficiently oversee the remediation and closure of plans of action and milestones[8] (POA&M) for system weaknesses. For example, CSAM contains 4920 open POA&Ms, and for 2915 of them (59 percent), the OAs did not set actual start dates for weakness remediation. Based on OMB metrics, DOT's Identify controls are at the Defined level of maturity, which is the second of the five levels.

2. **Protect.** DOT's Protect controls, which include identity and access management and security training, among other things, are not adequate. For example, the Department has set up multifactor user identity authentication for required access to only 39 out of 460 systems—approximately 8 percent of all DOT systems. Nine OAs had instances where inactive user accounts were not disabled within DOT policy timeframes. Furthermore, of over 600 facilities, FAA implemented use of personal identity verification (PIV) cards for physical access to only 89 (14 percent). The Department will not complete this implementation for its remaining facilities until fiscal year 2018. Lastly, the Department has allowed many employees to waive required annual security awareness and specialized training requirements in fiscal year 2016 due to what officials informed us was a problem with updating the training. Based on OMB metrics, DOT's Protect controls are at the Defined level of maturity, which is the second of the five levels.

3. **Detect**. The Department has implemented or is in the process of implementing its Detect controls, which are used to identify cybersecurity incidents, as part of its information security continuous monitoring (ISCM) program.[9] For example, each OA has a vulnerability weakness scanning tool for its systems. In addition, the Department is conducting a network wide assessment to further identify weaknesses in its common operating environment (COE) and to

[8] A plan, including completion dates, to correct and eliminate a system weakness.

[9] The ISCM program collects information in accordance with pre-established metrics, using information readily available in part through implemented security controls. ISCM maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

identify network assets. The Department is also tracking and updating outdated iOS software.[10] Still, there are weaknesses in the Detect area. In our sample of 75 systems, we found 33 (44 percent) that did not follow baseline configuration standards, had audit logs that had not been reviewed to determine what changes had occurred to systems' configuration settings, and/or the system was not scanned for weaknesses. Based on OMB metrics, DOT's Detect controls are in the Ad Hoc level of maturity, the lowest of the five levels.

4. **Respond.** DOT's Respond controls, which encompass incident handling and reporting, are not adequate. In a recent audit, we found that the Cyber Security Management Center's (CSMC) Security Operations Center (SOC), which handles cybersecurity incidents, did not have access to all departmental systems; access to Department network maps, or a ranking scheme to address incidents based on the seriousness of the risk they pose. Based on OMB metrics, DOT's Respond controls are in the Ad Hoc level of maturity, the lowest of the five levels.

5. **Recover.** DOT's Recover controls—for developing and implementing plans to restore capabilities and services impaired by cybersecurity incident—are not adequate. Several OAs do not maintain up-to-date contingency plans as called for by DOT and OMB requirements. These plans are meant to allow for the continuation of operations and services in the event of an emergency shut down. However, among our 75 sample systems, 9 OAs had deficiencies in their contingency plans and testing for at least 1 system, for a total of 67 systems (89 percent). Based on OMB metrics, DOT's Recover controls are at the Defined level of maturity, which is the second of the five levels.

We are making a series of recommendations to assist the Department in establishing and maintaining an effective information security program. See exhibit B for a list of open recommendations from our last six FISMA audits.

BACKGROUND

Under FISMA,[11] each Federal agency must make secure the information and information systems that support its operations, including those provided or managed by other agencies, contractors, or other entities. Similarly, OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, requires Federal agencies to ensure that appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. FISMA also requires each agency to report annually to OMB, Congress,

[10] iOS is the operating system used for mobile Apple devices, such as iPhone.
[11] 44 U.S.C. Chapter 35, Sub Chapter II, Information Security.

and the Government Accountability Office (GAO) on the effectiveness of its information security policies, procedures, and practices.

DOT's 11 OAs[12] manage the Department's 457 information systems (see exhibit C). The Department relies on these systems to carry out its missions, including safe air traffic control operations, qualified commercial drivers, and safe vehicles. DOT must also ensure the integrity of data in reports that account for billions of dollars used for major transportation projects such as highway construction and high-speed rail development.

For this year's review, OMB and DHS, in consultation with the Council of the Inspectors General on Integrity and Efficiency (CIGIE) and the Federal Chief Information Officers Council, revised the metrics[13] for inspectors general reviews. These metrics are now organized around the five security functions—Identify, Protect, Detect, Respond, and Recover—outlined in the National Institute of Standards and Technology's (NIST) cybersecurity framework.[14] See table 1 for definitions of these functions and the number of metrics in each function.

[12] In prior years, we reviewed 12 OAs. However, the Surface Transportation Board (STB) is no longer a part of DOT as a result of the STB Reauthorization Act of 2015. For purposes of this report, OST and OIG are treated as OAs. The 11 OAs are listed in exhibit C.

[13] *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, V1.1.3 September 26, 2016.

[14] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (2014).

Table 1. Cybersecurity Framework Functions and Definitions

Cybersecurity Framework Function	Definition	No. of FISMA metrics for 2016
Identify	Requires agencies to develop the understanding needed to manage security risks to systems, assets, data, and capabilities. Prior years' domains: risk management; contractor systems	21
Protect	Requires agencies to develop and implement appropriate safeguards to ensure delivery of infrastructure services. Prior years' domains: configuration management; identity and access management; security and privacy training.	31
Detect	Requires agencies to develop and implement processes to identify incidents that may include security breaches. Prior years' domain: Information security continuous monitoring.	49
Respond	Requires agencies to develop and implement processes for remediating detected cybersecurity incidents. Prior years' domain: Incident reporting.	54
Recover	Requires agencies to develop, implement and maintain up-to-date plans for restoration of capabilities and services impaired during a security event or emergency shut down. Prior years' domain: contingency planning.	11

Source: *FY 2016 Inspector General Federal Information Security Modernization Act of 2014. Reporting Metrics*, V1.1.3 September 26, 2016.

Furthermore, OMB provided inspectors general with guidance for determining the maturity of their agencies' security controls. In this guidance, OMB defined five maturity levels (see table 2) to help inspectors general categorize the maturity of their agencies' function areas and determine the effectiveness of the security programs. According to OMB, an effective program's maturity is at the managed and measurable level.

Table 2. Cybersecurity Maturity Levels and Definitions

Maturity Level (from lowest to highest)	Definition
Ad Hoc	Agency has not formalized the program and performs related activities in a reactive manner.
Defined	Agency has implemented comprehensive policies, procedures, and strategies consistent with Federal requirements and guidance.
Consistently Implemented	Policies, procedures and strategies are consistently implemented throughout the agency.
Managed and Measurable	Along with consistent implementation, activities are repeatable and use metrics to measure and manage the program's implementation, achieve situational awareness, control ongoing risk, and perform ongoing authorizations for system operation.
Optimized	In addition to being managed and measurable, the organization's program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and changing threat and technology landscape.

Source: *FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, V1.1.3 September 26, 2016.

Since 2001, we have published 15 reports that present the results of our evaluations of DOT's information security program and practices in accordance with FISMA requirements See exhibit F for a list of our previous reports.

IDENTIFY: DOT'S IDENTIFY FUNCTION CONTROLS ARE NOT ADEQUATE

DOT's Identify function controls, which include risk management and oversight of contractor systems, are inadequate. The Department does not have a comprehensive risk management program or a compliant weakness remediation program. Furthermore, some OAs' management of contractor-operated systems is not fully compliant and those with cloud systems have not executed agreements with their cloud services providers that cover system security. Based on OMB's metrics, DOT's Identify function is at the Defined maturity level.

DOT Does Not Have a Comprehensive Risk Management Program

FISMA requires agencies to ensure their information systems are secure to an acceptable level of risk. OMB requires agencies to implement risk management programs that include structures for managing and monitoring risk at the enterprise, business process, and system levels.[15] While it has risk management policy and procedures, the Department does not have a fully implemented program, including continuous authorization for system operation, management of

[15] OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, July 2016.

common controls, and weakness remediation. The lack of a comprehensive risk management program inhibits the Department's ability to establish a well working process for managing the risks associated with its operations and the use of Federal information systems.

The Department Has Not Completed Implementation of Its Risk Management Program

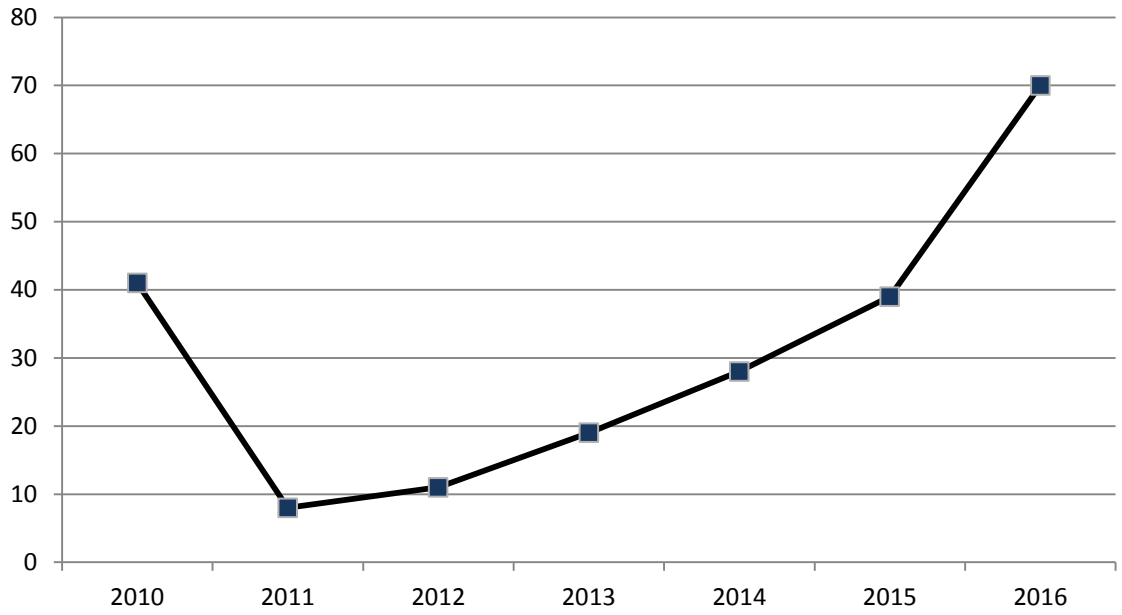
DOT has policies and procedures for risk management, but has not implemented an organizational structure to identify and communicate departmental risk to the OAs, leaving OAs to determine what risks they can accept or should address. FAA, FHWA, FMCSA, FRA, FTA, NHTSA, OIG, PHMSA and SLSDC have policies and procedures for their own risk management programs that include appropriate elements such as criteria for making risk based decisions. Last year, MARAD and OST informed us that they were drafting policies. This year, their policies were still in draft form and they did not identify plan target dates for completion.

The Department Continues To Operate Systems With Expired Authorizations

OMB Circular A-130, Appendix III requires Federal agencies to authorize their systems at least once every 3 years. An authorizing officer, usually a senior executive, reviews results of system security testing from the last authorization and reauthorizes the system when he or she determines that the system's operation poses an acceptable level of risk.

However, among the universe of 456 departmental systems, we found 70 systems that had expired authorizations to operate (see figure 1). In our 2015 review, we also found that 30 of these systems were unauthorized. This represents the fifth year of increases in systems that are not authorized to operate.

Figure 1. Number of Systems With Expired Authorizations to Operate Since 2010



Source: CSAM and OIG analysis.

These 70 systems belong to 7 OAs (see table 3).[16] We found that these OAs' information security system managers have not provided their authorizing officials with sufficient information to make risk-based decisions for reauthorization. Furthermore, the officials authorized extensions to operate for the systems without justifying their decisions.

Table 3. Systems Overdue for Reauthorization, by OA[a]

OA	Number of Systems
FAA	20
FHWA	11
FMCSA	10
FTA	1
MARAD	4
NHTSA	3
OST	21
Total	**70**

[a] As of June 30, 2016.
Source: OIG analysis.

[16] See table D-1 in exhibit D for a list of these 70 systems by name and OA.

Furthermore, for 61 of our 75 sample systems, the OAs did not follow departmental guidelines and authorized system operation without adequate support (see table 4). For example, in some instances, OAs did not complete security testing, reported inaccurate control testing results to CSAM, and identified security weaknesses that they did not report to CSAM. Based on our sample of 75 systems, we estimate that 372 of 453 systems, or 82 percent,[17] were operating with authorizations that were not fully supported. The lack of effective on-going security monitoring for system re-authorization makes it difficult for authorizing officials to make effective risk-based decisions.

Table 4. Results of OIG's Testing of Sample Systems' Security Controls

OA	Systems Tested	Systems Without Adequate Authorization to Operate
FAA	51	43
FHWA	3	0
FMCSA	2	2
FRA	2	1
FTA	2	2
MARAD	3	3
NHTSA	2	1
OIG	2	2
OST	6	5
PHMSA	2	2
Total	**75**	**61**

Source: OIG analysis.

DOT's Procedures for Monitoring Common Security Controls Are Insufficient

DOT continues to lack an effective process for OAs to assess, authorize, and monitor common security controls—controls that support multiple information systems. NIST requires providers[18] of these controls to (1) have policies and procedures for their use; (2) document the controls in security plans; (3) conduct continual assessments of the controls' security and monitor the controls' effectiveness; and (4) inform users when changes in the controls may adversely affect the protections the controls provide.

[17] Our 82 percent estimate has a margin of error of +/-5.7 percentage points at the 90 percent confidence level.
[18] A provider is anyone that has a system control used by another system.

As in previous years, DOT's common controls policy and procedures—which do not cover FAA's common controls—lack practices for monitoring and authorizing the controls. COE, FTA, and FAA did not provide us documentation to support their continual assessments of common controls. We found that COE and FTA personnel have not completed reauthorization assessments for the controls that they provide to customer agencies. Furthermore, COE and FAA personnel have not finalized guidance for customer agencies' use of the controls. This lack of comprehensive procedures and effective oversight of common controls could result in security incidents going undetected, unreported, or unresolved.

DOT's and OAs' Security Weakness Remediation Does Not Comply With All Requirements

Federal agencies must comply with several requirements in their remediation of security weaknesses. FISMA requires agencies to develop processes to remediate security weaknesses. OMB[19] requires agencies to develop POA&Ms for all weaknesses that they identify in their systems and to prioritize weakness remediation based on the seriousness of each weakness. A POA&M is a plan, including completion dates, to correct and eliminate a system weakness. DOT policy requires OAs to categorize their systems' weaknesses as low, medium, or high priorities based on their own criteria and to record POA&Ms in CSAM. Untracked and unresolved POA&Ms make it difficult for DOT to ensure systems are secured and protected.

The Department has 4920 open POA&Ms in CSAM—a 28 percent increase from 2015's 3830. We noted the following deficiencies with the 4920 POA&Ms (see table 5):

- 2915 POA&Ms, including 277 high priority and 1164 medium priority, did not have start dates, either planned or actual;
- 820, including 66 high priority and 260 moderate, did not document remediation costs;

[19] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones,* October 17, 2001.

Table 5. Summary of POA&Ms Opened Between 2009 and 2016 Without Actual Start Dates or Documented Remediation Costs, by OA

OA	Total open POA&Ms	Start dates left "TBD"	No documented costs
FAA	2733	1919	425
FHWA	42	41	0
FMCSA	873	22	26
FRA	117	89	21
FTA	129	0	0
MARAD	557	540	259
NHTSA	15	14	5
OIG	8	3	0
OST	382	251	84
PHMSA	52	35	0
SLSDC	12	1	0
Total	**4920**	**2915**	**820**

Source: CSAM POA&M report as of August 16, 2016.

We also found that the information on POA&Ms in CSAM for our sample systems was not complete. Specifically:

- For 57 of our 75 sample systems, the OAs did not submit POA&Ms on all identified security weaknesses to CSAM.
- FAA did not establish POA&Ms for control weaknesses identified in 185 audit recommendations for addressing security weaknesses in its air traffic control information security program that GAO made in a 2015 report.[20] As of September 8, 2016, FAA had closed only 12 of these recommendations. OCIO informed us that FAA is tracking these weaknesses outside of CSAM and would not complete the remediation until the end of fiscal year 2018.
- OCIO has not entered POA&Ms into CSAM for 22 open recommendations from our previous FISMA reports.
- FAA continues to report multiple weaknesses as one.

Incomplete information on POA&Ms in CSAM inhibits the abilities of the Department's CIO and Chief Information Security Officer's abilities to fully assess risk and funding requirements, analyze weakness trends, and implement departmentwide solutions.

[20] GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems*, GAO-15-221, January 2015.

Some OAs' Management of Contractor-Operated Systems Does Not Comply With Requirements

We found that FAA and other OAs' management of their contractor-operator systems did not comply with all requirements. Contractor operated systems are either fully or partially owned or operated by a contractor, another agency, or other entity. Contractor systems present unique risks because the Department frequently does not manage these systems' security controls.

FAA Has Not Correctly Categorized All of Its Contractor-Operated Systems

OMB requires agencies to identify each system's owner-operator—the agency itself, another agency, or a contractor—and designate each system as organization operated or contractor operated. We found that FAA has 122 contractor systems miscategorized as Agency operated systems, including 86 we identified in our 2015 review. According to FAA, the 122 systems should not be classified as contractor systems, but it did not provide justifications for not changing their classifications. The lack of accurate information on who operates its systems makes it difficult for DOT to provide direction to OAs and contractors on information security, to enforce compliance with information security requirements, and to ensure security risks are reduced.

OAs That Have Cloud Systems Have Not Executed Agreements With Their Cloud Services Providers That Cover Security

Cloud computing provides convenient access to computing resources that can be rapidly provisioned and released, including networks, servers, storage, and applications. Cloud computing resources are either private—for a single organization's exclusive use—or public, with infrastructure open to the general public. OMB requires agencies to identify all information systems that use cloud computing and ensure that the systems adhere to Federal cloud computing security requirements. These requirements are documented in OMB's Federal Risk and Authorization Management Program (FedRAMP). OMB's templates help agencies satisfy FedRAMP's requirements with standard language for contracts and service agreements with providers. One FedRAMP requirement calls for the OA to execute an agreement with the cloud services provider—in addition to the contract for cloud services—that delineates both the OA's and the services provider's responsibilities regarding system security.

The seven OAs—FAA, FTA, FRA, MARAD, PHMSA, OST, and NHTSA—that use cloud computing could not provide evidence they have complied with FedRAMP's requirements to execute agreements with their cloud services providers that clearly specify responsibilities for system security. Furthermore, during a recent audit of FTA's financial system applications, an OIG contractor also found that FTA does not have an agreement with its cloud services provider

that covers responsibilities for the security of the cloud systems. The lack of these agreements between OAs and their cloud services providers makes it difficult for the Department to ensure that service providers effectively manage the security of DOT's data in cloud systems.

PROTECT: DOT'S PROTECT FUNCTION CONTROLS ARE NOT ADEQUATE

DOT's Protect function controls, which include multifactor authentication and security awareness training, are not adequate. DOT has not transitioned all system applications and facilities to mandatory multifactor use identity authentication using PIV cards. We also found inactive user accounts that OAs had not disabled. Lastly, due to deficiencies in the Department's security training program, not all employees and contractors received required security awareness and specialized training. Based on OMB metrics, DOT's Protect function are at a Defined maturity level.

DOT Has Not Completed Implementation of the Use of PIV Cards for Access to System Applications and Facilities

OMB required that, by 2012, all Federal employees and contractors use PIV cards to login to agency computers and to access system applications. Use of PIV cards is part of multifactor user identity authentication which requires a computer system user to authenticate his or her identity with at least two unique factors possessed or known by the user. OMB also requires agencies to implement the use of PIV cards for access by both employees and contractors to departmental facilities.

In fiscal year 2015, OCIO informed us that 100 percent of the Department's employees with unprivileged accounts have received PIV cards and 98.3 percent of these cards have been configured for use in system access. OCIO also informed us that 100 percent of its privileged account[21] users have received PIV cards and 100 percent of these cards are configured for system access. However, according to CSAM as of May 2016, the OAs have transitioned only 39 of 460 systems to required use of PIV cards for application access. Regarding 421 systems that do not require use of PIV cards for application access, we found that: 140 are PIV enabled but do not actually require PIV cards for access.

- OCIO officials could not explain why 237 systems were not enabled for PIV card access to applications, and did not provide explanations, such as technical

[21] An unprivileged user utilizes an account for everyday access to applications such as email and data processing. A privileged user is authorized and trusted to perform security-relevant functions that ordinary, or unprivileged, users are not authorized to perform.

incompatibility.

- 140 contain personally identifiable information.
- For 44 systems, CSAM information does not specify the status of PIV card use for application access. According to OCIO officials, the OAs have created POA&Ms in CSAM to document these systems' conversion to PIV access for applications.

After we notified them about these matters, OCIO officials informed us that OCIO will develop a PIV oversight cybersecurity action memorandum that directs the OAs to update these POA&Ms within 60 days of memo issuance, but did not indicate an issuance date. See table 6 for a summary by OA of application access by PIV card.

Table 6. Summary of Information in CSAM on OAs' Use of PIV Cards for Application Access

DOT Systems			Use of PIV card for access is specified as:			
OA	FIPS[a] Category	Number of Systems	Required	Enabled but not required	Not enabled	Unspecified
FAA		**318**	**13**	**93**	**208**	**4**
	High	21	2	15	4	0
	Moderate	207	9	60	136	2
	Low	90	2	18	68	2
FHWA		**18**	**0**	**16**	**2**	**0**
	High	5	0	5	0	0
	Moderate	13	0	11	2	0
	Low	0	0	0	0	0
FMCSA		**18**	**11**	**3**	**4**	**0**
	High	0	0	0	0	0
	Moderate	18	11	3	4	0
	Low	0	0	0	0	0
FRA		**11**	**0**	**0**	**2**	**9**
	High	0	0	0	0	0
	Moderate	8	0	0	1	7
	Low	3	0	0	1	2
FTA		**9**	**2**	**3**	**0**	**4**
	High	0	0	0	0	0
	Moderate	9	2	3	0	4
	Low	0	0	0	0	0
MARAD		**17**	**0**	**14**	**2**	**1**
	High	0	0	0	0	0
	Moderate	12	0	10	1	1
	Low	5	0	4	1	0
NHTSA		**17**	**6**	**0**	**3**	**8**
	High	0	0	0	0	0
	Moderate	13	4	0	2	7
	Low	4	2	0	1	1

DOT Systems			Use of PIV card for access is specified as:			
OA	FIPS[a] Category	Number of Systems	Required	Enabled but not required	Not enabled	Unspecified
OIG		**2**	**2**	**0**	**0**	**0**
	High	0	0	0	0	0
	Moderate	2	2	0	0	0
	Low	0	0	0	0	0
OST		**42**	**1**	**11**	**15**	**15**
	High	6	1	1	3	1
	Moderate	30	0	9	10	11
	Low	6	0	1	2	3
PHMSA		**7**	**4**	**4**	**0**	**3**
	High	0	0	0	0	0
	Moderate	3	3	0	0	0
	Low	4	1	0	0	3
SLSDC		**1**	**0**	**0**	**1**	**0**
	High	0	0	0	0	0
	Moderate	0	0	0	0	0
	Low	1	0	0	1	0
Total Systems		**460**	**39**	**140**	**237**	**44**
Total High		32	3	21	7	1
Total Moderate		315	31	96	156	32
Total Low		113	5	23	74	11

[a] Federal Information Processing Standards (FIPS) document processing, encryption, and other information technology for non-military agencies and Government contractors and vendors.
Source: CSAM as of May 23, 2016.

We also found that DOT has begun to deploy virtual desktop infrastructure (VDI) without the required use of PIV cards for access. A VDI enables a user to have a DOT server replicate his or her desktop on devices in addition to his or her Government-issued computer. Officials in OCIO, which oversees the COE, informed us that technical and financial challenges have delayed full implementation of mandatory use of PIV cards for VDI access, and plan to resolve the issues by December 2016.

Furthermore, as we found in 2015, the Department has not implemented the use of PIV cards for physical access to all of its facilities. For example, FAA has implemented PIV card access at only 89 of 618 (14 percent) facilities. FAA officials informed us that the Agency plans to make all FAA facilities require the use of PIV cards for access by the end of fiscal year 2018. See table 7 for details on FAA's conversion of the remaining 529 facilities to PIV card access. As seen in the table, FAA will not convert 18 high risk facilities to mandatory PIV card access until 2018.

Table 7. FAA's Plan To Enable Facility Access With PIV Cards

Fiscal Year	Facilities by Risk Rating Level[a]			
	I	II	III	IV
16	0	92	13	0
17	4	192	9	0
18	0	163	38	18
Sub-Total	**4**	**447**	**60**	**18**
Total		**529**		

[a] FAA rates each facility with a level of risk for compromise. A **Level I** facility has a risk rating of **minimum** because it has low levels of contact with the public. A **Level II** facility has a risk rating of **low** because it houses fewer than 100 Federal employees, contains 10,000 square feet or less, has moderate levels of contact with the public, and Federal activities that occur there are routine in nature similar to commercial activities. A **Level III** facility has a risk rating of **medium** because it houses between 101 and 250 Federal employees, contains between 10,000 and 100,000 square feet, has moderate to high levels of contact with the public, and tenant agencies that may work in law enforcement or court-related agencies and functions, and manage Government records and archives. A **Level IV** facility has a risk rating of **High** because it houses 251 to 750 Federal employees, contains between 100,000 and 250,000 square feet, and has high levels of contact with the public, and tenant agencies that may do high-risk work in law enforcement and intelligence, courts, judicial offices, and highly sensitive Government records.
Source: FAA.

This lack of use of PIV cards for access to the Department's system applications and facilities makes it difficult for DOT to be sure that system users and individuals that access departmental facilities are correctly identified as authorized personnel.

In Some Instances, DOT Did Not Close Inactive Accounts Within Required Timeframes

DOT's account management controls for the networks that service approximately 73,000 of the Department's accounts have allowed a few accounts to remain accessible after long periods of inactivity instead of being close according to DOT policy. To minimize the risk that individuals who should no longer have access will gain unauthorized access to information and systems, DOT's cybersecurity policy requires system administrators to close, or disable, user accounts after the users' separation from DOT or when the account is inactive based on the time period specified by the DOT Component. However, we found 132 inactive user accounts that had not been disabled, up from last year's 57 accounts by 57 percent. See table 8 for a summary of inactive accounts by OA.

Table 8. Summary of Inactive Accounts That Were Not Disabled as of June 30, 2016

OA	Days of account inactivity:		
	> 120 Days	**> 90 Days**	**Total**
FAA	83	18	101
FHWA	2	0	2
FMCSA	2	0	2
FRA	3	3	6
FTA	0	2	2
PHMSA	5	0	5
MARAD	7	0	7
OST	4	0	4
SLSDC	3	0	3
Total	**109**	**23**	**132**

Source: OIG analysis.

When we informed the OAs of these inactive accounts, we learned the following:

- FAA officials informed us that 15 of the Agency's 101 inactive accounts were air traffic control (ATC) network accounts that were on its list of accounts exempt from disabling. FAA does not disable some inactive accounts, including ATC accounts, for several reasons and maintains these accounts and their users' profiles on its "exemption list." However, FAA officials later informed us that the 15 accounts were actually not on the exemption list, that all 101 inactive accounts had been disabled, and that they are evaluating the Agency's user account management process.
- FRA officials informed us that they disabled the six inactive user accounts we found and are currently working to improve its account disabling process.
- MARAD officials reported to us that the Agency's network administrators did not properly change the status of two of seven inactive accounts we found. The remaining five accounts were disabled.
- OST officials reported they could not verify the status of one account we found to be inactive and the users of another three were DOT employees who eventually logged on.
- NHTSA informed us that one account was still active and disabled four inactive accounts.
- SLSDC officials stated that the users of the three accounts were current employees, but we found that these accounts were inactive and should be disabled.

DOT Has Inappropriately Exempted Some OAs From Security Awareness and Privacy Training, and Some OAs Did Not Meet Specialized Training Requirements

FISMA requires agencies to develop and maintain a security training program to ensure that all computer users are adequately trained in their security responsibilities before they are allowed access to agency information systems. Furthermore, both FISMA and OMB require agencies to provide security awareness training to all employees and contractors, even those that never access computer systems.

However, OCIO officials informed us that because of a problem with updating the security awareness training content for fiscal year 2016, they approved OAs' application of employees' completed fiscal year 2015's training to the training requirement for fiscal year 2016. Consequently, not all personnel that reported meeting the 2016 requirement actually completed training.

Furthermore, DOT's cybersecurity policy requires OAs to provide specialized training for personnel that perform certain security related roles. The policy specifies which roles require annual specialized training, and previously defined the minimum number of hours required for each role. In 2016, OCIO released guidance that introduced a change in departmental requirements for specialized training. OA personnel are no longer required to annually complete a specified number of hours in specialized training. Instead, they have to complete training courses on areas of specialization in the National Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education. The Framework lists and defines 32 specialty areas in cybersecurity work and identifies common tasks and knowledge, skills, and abilities associated with each area. OCIO's guidance calls for the OAs to determine which personnel work in the Framework's specialized areas and to then require them to complete annual training on their areas.

However, we found issues with the OAs' specialized training:

- OST could not provide evidence that personnel that required specialized training actually completed it;
- MARAD did not track its employees' completion of specialized training.
- FTA, SLSDC, FMCSA, the Volpe Center, and NHTSA provided information on their employees' training but not on how employee roles related to the Framework's specialized areas or which competencies each training course covered.
- FAA's information on its employees did not indicate in what fiscal year the employees completed the specialized training.

Lack of regular security awareness training could result in behaviors that put DOT's information at risk, such as e-mail abuse, incorrect user ID and password development, and internet misuse. Furthermore, the lack of specialized training for employees with security related duties makes it difficult for DOT to be sure that its personnel have the needed knowledge, skills, and abilities to protect the Department's information.

DETECT: DOT'S DETECT FUNCTION CONTROLS ARE NOT SUFFICIENT

The Department has implemented or is in the processing of implementing its Detect function controls—which are used to identify cybersecurity incidents—including its information security continuous monitoring (ISCM) program. However, the ISCM program lacks: (1) a complete inventory of hardware and software; and (2) fully automated and integrated configuration setting management and common vulnerability management. Based on OMB's metrics, DOT's Detect function is at the Ad Hoc maturity level.

Major Initiatives in Process To Improve Detect Controls

The Department launched several initiatives to enhance its Detect controls, including ISCM:

- OCIO initiated an enterprise (excluding FAA) assessment, including both wired and wireless networks. According to OCIO, this critical effort is mapping and capturing necessary information on infrastructure devices.
- Each OA now has a vulnerability scanning tool for its systems. They also have personnel assigned to run these tools.
- The Department has implemented, for DOT Headquarters, DHS's updated Einstein tool, which provides intrusion detection support.
- In September 2016, the OCIO initiated a major, aggressive initiative to mitigate critical vulnerabilities on Apple devices using the iOS operating systems. At present, the OCIO is reporting that 4,472 devices have been assessed and patched.

If completed properly, these initiatives will increase DOT's ability to detect and mitigate attempts to compromise its cybersecurity.

DOT's Inventories of Its Hardware and Software Assets Are Incomplete

As in 2015, we found that the Department's inventories of both its hardware and software assets were incomplete. NIST standards and DOT's security policy require OAs development and documentation of a complete inventory of system

components, devices, and software that is regularly updated as installations, removals, and software updates occur. The OAs must also update OCIO on the current inventories on a quarterly basis. OCIO then reports to OMB.

However, DOT lacks a process for accurately tracking its IT assets. We found that the hardware inventory listed in OCIO"s most recent quarterly report[22] to OMB did not match the OAs' individual inventories. Furthermore, FAA and the Volpe Center[23] informed us that they are unable to provide an accurate list of hardware assets. OCIO informed us that the Department owns 31,639 hardware assets but the OAs reported 81,339. Furthermore, the inventories the OAs provided to us included workstations and servers but not other devices such as routers. Table 9 summarizes DOT's hardware inventory.

Table 9. Summary of DOT's Hardware Assets

Operating Administration	Inventory[a]	
	From OCIO	From the OA
FAA	Not provided	51,376
FHWA	4,027	4,027
FMCSA	4,013	4,013
FRA	5,141	2,947
FTA	2,469	2,469
MARAD	2,482	2,482
US Merchant Marine Academy	Not provided	Not provided
NHTSA	2,992	2,992
OIG	Not provided	702
OST	4,776	4,776
Common Operating Environment	Not provided	Not provided
Volpe Center	3,320	3,136
PHMSA	2,419	2,419
SLSDC	Not provided	Not provided
Totals	**31,639**	**81,339**

[a] As of April 2016.
Source: OIG analysis.

The Department's inventory of its software assets is also incomplete. OCIO has not provided the OAs with guidance on what data they must provide to OCIO on their software assets. We found that:

[22] Chief Information Officer 2016 Quarter 3 FISMA Report.
[23] *The Volpe Center's Information Technology Infrastructure is at Risk for Compromise*, OIG Report Number FI-2016-056, March 22, 2016.

- FHWA, FTA, MARAD, NHTSA, OST, PHMSA, and FMCSA's software inventories did not include the dates the inventories were taken so we could not verify the lists' accuracy.
- OCIO has not set a frequency for the OAs' reports to it on their assets. As a result, the OAs' reporting frequency varied. Some report monthly while others report only annually.

This lack of complete IT asset inventory inhibits the Department's ability to monitor its systems' security and puts the systems at risk for unauthorized access and compromise.

DOT Has Not Fully Automated and Integrated Configuration Setting Management and Common Vulnerability Management

In addition to management of hardware and software assets, information security continuous monitoring requires the development and implementation of configuration setting management (CSM) and common vulnerability management (CVM).

- **CSM.** Software and hardware products have default settings—such as password lengths and characters—that their designers establish. Because they can be easily hacked by individuals that want to gain unauthorized access to a system, default settings must be changed—or reconfigured—when the product is implemented so that the system remains secure. CSM is the process by which system administrators change default settings to meet their agencies' security standards. As requirements or standards change, an administrator will adjust the settings to comply.
- **CVM.** Throughout the life of software and hardware products, users discover security weaknesses. The products' designers develop patches to remediate these weaknesses that the product users must apply to their systems. If patches do not exist, administrators must monitor the status of each vulnerability and identify compensating controls.

NIST's SP 800-137 and OMB's M-14-03 require agencies to automate CSM and CVM, but OCIO is not requiring the OAs to follow NIST's and OMB's guidelines. For example, as a result of recent monitoring, OCIO found 110,794 weaknesses on 19,790 departmental computers.[24] However, OCIO officials did not provide information on which system each weakness impacted to help the affected OAs prioritize weakness remediation. Furthermore, we found 62 weaknesses in 33 of our 75 sample systems for which the OAs have not implemented correct

[24] Excluding FAA's and the Volpe Center's.

configuration settings or completed corrective actions.[25] Unremediated system weaknesses and lack of data for remediation prioritization exposes the Department's networks and information systems to compromises that could result in loss, damage, and misuse of data and other valuable assets.

RESPOND: DOT'S RESPOND FUNCTION CONTROLS ARE NOT SUFFICIENT

DOT's Respond controls, which address incident handling and reporting, are not sufficient, and based on OMB's metrics, the function is at the Ad Hoc maturity level. Under FISMA, OMB policy, and NIST guidelines, departments must establish incident response and reporting programs for their information systems. According to DOT policy,[26] when an incident such as a security breach or interruption of service occurs, the OA must report the incident to CSMC which then analyzes the incident, categorizes it, and reports it to the United States Computer Emergency Readiness Team (US-CERT) at DHS. DOT policy also requires CSMC to have full network visibility over all DOT systems, including systems operated on behalf of the OAs by contractors and other Government organizations.

During our recent cybersecurity incident handling audit, we found that CSMC's security operations center, which handles cybersecurity incidents, did not have access to all departmental systems or network maps, or a ranking scheme to address incidents based on the seriousness of the risk they pose. Furthermore, as in our 2015 FISMA review, we found that the OAs do not comply with all FISMA and DOT requirements. Specifically:

- Officials at FMCSA, NHTSA, and OST informed us that their Agencies have not developed metrics to assess the effectives of their incident response program. FMCSA officials indicated that they plan to work with the COE to evaluate the effectiveness of the Agency's incident handling and reporting program.

- MARAD officials informed us that they are revising a draft policy for incident reporting and will finalize it the end of fiscal year 2016.

- OCIO officials informed us that they are in the process of reauthorizing the COE for operation. This reauthorization process includes the COE's common controls for incident handling and reporting. OCIO officials further informed

[25] See table E-1 in exhibit E for a list of the weaknesses we identified.
[26] Department of Transportation Office Of The Chief Information Officer Cyber Security Incident Response Plan, March 2014.

us that re-authorization should be completed by December 31, 2016. Until then, OCIO cannot demonstrate that the COE has visibility of all network interfaces and devices for incident handling.

The lack of an effective incident response program makes it difficult for the Department to be sure that as many cybersecurity incidents as possible are detected and reported to US-CERT. Furthermore, unreported incidents inhibit DHS's ability to ensure that Federal systems and information are secure from compromise.

RECOVER: DOT'S RECOVER FUNCTION CONTROLS ARE INADEQUATE

DOT's Recover function control for contingency planning is not adequate, and based on OMB's metrics, is at a Defined level of maturity. OMB, NIST, and DOT policy require agencies to establish and periodically test contingency plans[27] for continuation of operations and services, including those provided by information systems, in the event of an emergency shut down. They also require that agencies test and update their contingency plans at least annually.

However, among our 75 sample systems, 9 OAs had deficiencies in their contingency plans and testing for at least 1 system.[28] We found that 67 systems in our sample (89 percent) did not meet OMB and FISMA requirements for contingency planning and testing. Based on our sample of 75 systems, we estimate that for 391 of 453 systems, or 86.3 percent, the OAs did not perform effective contingency planning or testing.[29] See table 10 for a summary of the deficiencies in contingency planning that we found.

[27] A contingency plan contains policy and procedures for an agency's response to a perceived loss of mission capability and used by risk managers to determine what happened, why, and what to do. The plan may point to the continuity of operations plan (COOP) or disaster recovery plan for major disruptions. A disaster recovery plan (DRP) details the recovery of one or more information systems at an alternative facility in response to a major hardware or software failure or destruction of facilities. A business continuity plan documents a predetermined set of instructions or procedures for how an agency will sustain mission and business functions during and after a significant disruption.

[28] We reviewed additional systems as part of a separate audit on contingency planning and will provide further details on these systems in our report on that audit.

[29] Our 86.3 percent estimate has a margin of error of +/- 4.9 percentage points at the 90 percent confidence.

Table 10. Summary of Deficiencies in OAs Contingency Planning and Testing for Sample Systems

Contingency Planning Requirements	FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OIG	OST	PHMSA
Business Continuity and Disaster Recovery Plan (BCDRP)	X	X	X	X	X	X	X	✔	X	X
BCDRP revised to correct deficiencies found during testing	X	X	X	X	X	X	X	✔	X	X
Contingency plans tested	X	✔	X	✔	X	X	X	✔	X	X
Contingency test after-action report developed	X	X	X	✔	X	X	✔	✔	X	X
System backup in accordance with procedures	X	X	X	✔	X	X	✔	✔	X	X
Alternate processing sites defined	X	✔	X	✔	X	X	✔	NT	X	X
Supply Chain Threat[a] Tested	X	X	NT	NT	NT	NT	NT	NT	NT	NT

[a] The threat that critical replacement parts and services will not be available after an emergency shut down.
NT—Not tested.
Source: OIG analysis.

A lack of effective contingency planning and testing makes it difficult for the Department to ensure continuous operations in the event of a disaster or a disruption of service.

CONCLUSION

A secure information network ensures that operations across the Government are carried out efficiently and effectively. For DOT, secure systems are also critical to ensuring public safety—the Department's foremost mission. While DOT is in process of implementing several initiatives, we continue to find that many of its information security controls are deficient. In some security areas, such as authorizing systems to operate and security training, deficiencies are increasing. Until DOT takes action to remediate these deficiencies, the Department's information systems will continue to be at increased risk of attack or compromise.

RECOMMENDATIONS

To help the Department address the challenges in developing a mature and effective information security program, we recommend that the Deputy Secretary, or his designees, take the following actions in addition to the 18 recommendations that are still open from prior FISMA reports.

1. Work with all OAs to complete expired authorizations and reinforce or strengthen policy requiring systems be reauthorized prior to their expiration dates.
2. Work with all OAs to perform a thorough CSAM quality review to ensure system documentation matches what is entered into CSAM. At a minimum, the review should verify that: (1) system authorization dates in CSAM match what is approved by the authorizing official; (2) POAMs are created and reported once a security weakness is found; and (3) authorizing officials are provided accurate documentation on all risks accepted.
3. Work with FAA, FHWA, FMCSA, FTA, MARAD, NHTSA, and OST to develop risk acceptance memos for the expired systems identified in this report.
4. Work with OST COE, FTA, and FAA, the common control providers, to report and update risk acceptance for shared controls that are not implemented in DOT's Repository (e.g., CSAM) per FISMA, OMB, and DOT requirements.
5. Work with FAA and require them to review CSAM POA&M entries, and identify and correct cases where multiple weaknesses were entered as one.
6. Perform a review of CSAM POA&Ms and assess if the entries are compliant with DOT policy. For deficient data, require OAs to provide a corrective action plan.
7. Identify and document OST COE compensating controls when used to address security weaknesses in CSAM and system authorizations.
8. Report/update OST COE security weaknesses found during vulnerability assessments in DOT's Repository (e.g., CSAM) per FISMA, OMB, and DOT requirements.

AGENCY COMMENTS AND OIG RESPONSE

We provided the Department with our draft report on October 11, 2016, and received its response—included as an appendix to this report—on November 4, 2016. The Department concurred with recommendations 1 through 4 and 6, as written. The Department further indicated that it will provide a corrective action plan to address these recommendations within 60 days of report issuance. We therefore consider these recommendations open and unresolved.

The Department did not concur with recommendations 5, 7 and 8, which involve addressing, recording, and tracking security control weaknesses. DOT objected to the criteria we applied in recommendation 5 and proposed alternative actions for recommendations 7 and 8. We disagree with DOT's position on the criteria for recommendation 5 and are extremely concerned that the alternatives proposed will be insufficient especially given the Department's history of poor performance in

the management of its POA&Ms. As noted in our report, the Department has 4920 open POA&Ms in CSAM—a 28 percent increase from 2015's 3830. In addition, our testing demonstrates that DOT cannot ensure that CSAM captures all of DOT's known cybersecurity weaknesses. Excessive weaknesses—that number in the thousands—and incomplete tracking are problems that have recurred in each of our last 9 annual FISMA reports.

The following specifically addresses each nonconcurrence:

- DOT did not concur with recommendation 5 to require FAA to review POA&Ms in CSAM, and identify and correct cases in which multiple weaknesses were entered as one, stating that this is neither a Federal nor DOT requirement and represents unnecessary complexity and inefficiencies. We disagree. DOT's Security Weakness Management Guide, dated September 2013, states "each system weakness is entered individually on a system-specific POA&M in CSAM." It further states that "a system weakness arises from a specific management, operational, or technical control deficiency."
- DOT did not concur with recommendation 7 to identify and document OST-COE's compensating controls used to address security weaknesses, stating that the Department proposes instead that to reinforce system owner responsibilities through additional guidance regarding documentation and implementation of controls. We disagree with the Department's position. This responsibility to identify and document OST-COE's compensating controls is shared by three parties: COE management who develops and provides the controls); the system owners, who use the controls' and OCIO who is responsible for DOT cybersecurity. However, although the responsibility is shared, system owners must rely on OST-COE management to identify compensating controls prior to using them.
- DOT did not concur with recommendation 8 to report/update OST-COE's security weaknesses found during vulnerability assessments in DOT's repository, stating that neither Federal nor DOT policy require tracking of discrete technical vulnerabilities as individual POA&Ms and that doing so would be highly inefficient and burdensome. We maintain that tracking of individual vulnerabilities is required and request clarification on what the Department meant when it referred to "discrete" vulnerabilities. OMB M-04-25 states that "POA&Ms must include all security weaknesses found during any review done by, for, or on behalf of the agency, including…critical infrastructure vulnerability assessments." DOT policy further requires critical, high and medium technical vulnerabilities to be either remediated or entered into POA&Ms within 90 days. In its response, the Department also proposed to address our findings by focusing on the effectiveness of the OAs' vulnerability management programs. We disagree with this proposal given issues that have occurred at DOT with these programs. For example, recently, a key component

of the Department's vulnerability management tools experienced a systemwide failure due to a database corruption issue that rendered the component inoperable and in need of rebuilding.

Given the importance of addressing, recording, tracking, and resolving security control weaknesses, we consider these recommendations open and unresolved and request that the Agency reconsider its position.

Finally, in its response, the Department characterizes DOT's cybersecurity program as "FISMA compliant" and disagrees with our overall assessment that the program is ineffective. We recognize the positive steps taken by the Department such as its recent network assessment, but emphasize that our assessment is based on OMB metrics that require that effective programs meet a range of challenging criteria including consistent compliance with requirements. Our report discloses numerous deficiencies that constitute non-compliance with FISMA and based on OMB metrics, an ineffective information security program. For example, as of June 30, 2016, 70 of 450 systems were not authorized to operate as required, and DOT did not meet the basic requirement for annual security awareness training in 2016 due to a glitch in its training system. We will continue to assess DOT's program under the OMB metrics in order to provide timely and useful information for the Department as it seeks to further improve it cybersecurity program.

ACTIONS REQUIRED

We consider recommendations 1 through 4 and 6 open and unresolved until receipt and review of the corrective action plan. In accordance with DOT Order 8000.1C, we request DOT reconsider its position for recommendations 5, 6 and 8 and provide its response within 30 days of the date of this report.

We appreciate the courtesies and cooperation of the Department's representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1959, or Louis C. King, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1407.

#

cc: Assistant Secretary for Budget and Programs/Chief Financial Officer
CIO Council Members
DOT Audit Liaison, M-1

EXHIBIT A. SCOPE AND METHODOLOGY

We conducted our audit between January and October 2016, in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Generally accepted Government auditing standards also require us to disclose impairments of independence or any appearance thereof. OMB requires that the FISMA template include information from all OAs, including OIG. Because OIG is a small component of the Department, based on number of systems, any testing pertaining to OIG or its systems does not impair our ability to conduct this mandated audit.

FISMA requires us to perform annual independent evaluations to determine the effectiveness of DOT's information security program and practices. FISMA further requires that our evaluations include testing of a subset of systems, and an assessment, based on our testing, of the Department's compliance with FISMA and applicable requirements.

To meet FISMA and OMB requirements, our objective would determine the effectiveness of DOT's information security program and practices for the 12-month period between July 1, 2015, and June 30, 2016. Per OMB's Annual Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, agencies should set cut-off dates for data collection and report preparation that allow adequate time for meaningful internal reviews, comments, and resolution of disputes before reports' finalization. OCIO agreed to use a cutoff of June 30, 2016. We obtained a listing with 456 computer systems that had not been reviewed within the last 3 years from the Department's CSAM on January 29, 2016. We stratified this universe into 22 strata by FAA Lines of Business and Operating Administrations. We computed sample sizes proportionately with a minimum of 2 from each stratum unless there was only one, and selected a stratified simple random sample of 75 out of 456 computer systems. During our audit we found that one system was decommissioned. When estimating, we reduced our universe proportionately to 453 to account for the decommissioned system. Our sample design allowed us to estimate the percentage and number of compliant systems with NIST and DHS requirements in the following areas: risk categorization; security plans; annual control testing; contingency planning; certification and accreditation; incident handling; and plans of actions and milestones with a precision no greater than +/-8.2 percentage points

at the 90-percent confidence level. See table A-1 for sampled systems and table C-1 for the system inventory.

We evaluated prior years' recommendations and supporting evidence to determine what progress had been made in the following areas: continuous monitoring; configuration management; contingency planning; risk management; security training; contractor services; and identity and account management. We also conducted testing to assess the Department's device inventory; its process for resolution of security weaknesses; configuration management; incident reporting; security awareness training; remote access; and account and identity management. Our tests included analyses of data contained in CSAM, reviews of supporting documentation, and interviews with departmental officials.

As required, we submitted to OMB qualitative assessments of DOT's information security program and practices. We conducted our work at departmental and OA Headquarters' offices in Washington, D.C.

Table A-1. OIG's Representative Subset of Systems by OA

	System	Impact Level[a]	Contractor System[b]
Federal Aviation Administration			
1	Quality Center Automated Testing (QCAT)	Moderate	N
2	CWP (Corporate Work Plan)	Moderate	N
3	Enterprise Mobile Device Management System	Moderate	N
4	Information Technology Asset Management System	Low	N
5	FDR (Federal Data Registry)	Low	N
6	Documentum Shared Service	Moderate	N
7	ATO Network	Moderate	N
8	REMS (Real Estate Management System)	Moderate	N
9	AWA ARCHIBUS	Low	N
10	PIPS (Payroll Imaging Process Services)	Moderate	N
11	BMX (Business Management Solutions)	Low	N
12	EASE (Enterprise Architecture & Solutions Environment)	Moderate	Y
13	ACSMS (Aeronautical Center Security Management System)	Moderate	N
14	Matter Tracking Information System	Moderate	N
15	iConect	Moderate	N

System		Impact Level[a]	Contractor System[b]
16	OVLTP (Online Voluntary Leave Transfer Program)	Moderate	N
17	LERIS (Labor and Employee Relations Information System)	Moderate	Y
18	LabNet (William J. Hughes Technical Center Network)	Moderate	N
19	AKCS (Access Key Credentialing System)	Moderate	N
20	Aviation Environmental Design Tool	Moderate	N
21	SOAR (System of Airport Reporting)	Moderate	N
22	CATS (ARP) (Certification Activity Tracking System)	Moderate	N
23	ASH Web Portals (FSRS, PASS, WEB-DG, IMS, ASH SAVI) Applications	Moderate	N
24	ITS (Investigative Tracking System, also includes DUI/DWI Driving Under the Influence/Driving While Intoxicated System	Moderate	N
25	ECG/EBUS (En Route Communications Gateway/Enhanced Back Up Surveillance)	Moderate	N
26	FAVES (FAA Administrative Voice Enterprise Services)	Low	Y
27	WSP (Weather System Processor)	Moderate	N
28	ASTI (Alaskan Satellite Telecommunications Infrastructure)	Moderate	N
29	National Defense Program	Moderate	N
30	SWIM Terminal Data Distribution System	Moderate	N
31	VOLMET (Volatile Meteorological System)	Low	N
32	SWIMLAB (System Wide Information Management Laboratory)	Low	N
33	WAAS (Wide Area Augmentation System)	Moderate	N
34	ASOS (Automated Weather Sensors System)	Low	N
35	FDIO (Flight Data Input/Output)	Low	N
36	ETVS (Enhanced Terminal Voice Switch)	Moderate	N
37	Runway Status Lights	Low	N
38	AMASS (Airport Movement Area Safety System)	Moderate	N
39	Enterprise Management Tool Suite	Moderate	N
40	Environment and Occupational Safety and Health Training Needs	Low	N

System		Impact Level[a]	Contractor System[b]
41	NASPAS (National Airspace Performance Analysis System)	Low	N
42	Procurement Automated Tracking System Financials (PATS Financials)	Low	N
43	FAA Workplace Inspection Tool (WIT)	Low	N
44	AOV Facility Specific Safety Standard	Low	N
45	DRS (Designee Registration System)	Moderate	N
46	eFSAS (Enhanced Flight Standards Automation System)	High	N
47	VDRP (Voluntary Disclosure Reporting Program)	Moderate	N
48	110A (110A Inspector Credentials System)	High	N
49	RBRT (Risk Based Resource Targeting)	Moderate	N
50	Designee Management System	Moderate	N
51	MSAD (Monitor Safety Analyze Data)	Moderate	N
Federal Highway Administration			
52	Federal Lands Labor Cost Distribution Process	Low	Y
53	Rapid Approval & State Payment System	High	Y
54	Information Technology Division General Support System	High	Y
Federal Motor Carrier Safety Administration			
55	A&I-NCCDB-DataQs	Moderate	N
56	FMCSA Service Centers	Moderate	N
Federal Railway Administration			
57	Automated Track Inspection Program	Moderate	Y
58	Railroad Credit Assessment and Portfolio Management System	Low	N
Federal Transit Administration			
59	Transportation Electronic Award Management System	Moderate	Y
60	National Transit Database Next Generation	Moderate	Y
Maritime Administration			
61	Ship Manager Performance Evaluation and Appraisal System	Moderate	Y
62	MARAD Internet	Moderate	Y
63	Maritime Service Compliance System	Moderate	Y

	System	Impact Level[a]	Contractor System[b]
National Highway Transportation Safety Administration			
64	NHTSA301: Teleprocessing & Timesharing Services NDR Program	Moderate	Y
65	NHTSA026: Motor Vehicle Importation System	Moderate	N
Office of Inspector General			
66	Computer Crimes Unit Network	Moderate	N
67	US DOT OIG Infrastructure	Moderate	N
Office of the Secretary of Transportation			
68	Electrical Metering System	Low	Y
69	Departmental Office of Civil Rights Disadvantage Business Enterprise and Airport Concession Ineligibility Database	Moderate	Y
70	Volpe Centralized Data Repository	Moderate	Y
71	Case Tracking System	Moderate	Y
72	Investigative Tracking System (ITS)	Moderate	Y
73	Consumer Complaints Application	Moderate	Y
Pipelines and Hazardous Materials Safety Administration			
74	PHMSA Portal System	Moderate	Y
75	National Pipeline Mapping System	Low	Y

Legend: N = No Y = Yes

[a] NIST defines impact levels based on the effect a breach of security could have on a system's confidentiality, integrity and availability. If the effect is limited, the impact level is low; if serious, moderate; if severe, high.
[b] DOT's definition of contractor system.
Source: OIG analysis.

EXHIBIT B. STATUS OF PREVIOUS YEARS' RECOMMENDATIONS

Table B-1. Open Recommendations, Fiscal Years 2015-2009

Fiscal Year 2015; OIG Report Number FI-2016-001	
Number	**Recommendation**
1	The Deputy Secretary, or his designees, take action to ensure that the OCIO revises the Department's Cybersecurity policy to document exclusions for PIV required use for network and system access.
2	The Deputy Secretary, or his designees, take action to work with the OAs to develop a formal transition plan to the proposed ISCM target architecture that includes but is not limited to: (1) continuously assessing security controls; (2) reviewing system configuration settings; and (3) assessing timely remediation of security weaknesses. During the transition period, establish processes and practices for effectively collecting, validating, and reporting ISCM data.
3	The Deputy Secretary, or his designees, take action to ensure that FAA, FHWA, FMCSA, FRA, FTA, NHTSA, MARAD/USMMA, OST, and SLSDC perform actions to immediately disable user accounts that have been inactive for over 90 days, as required by the DOT compendium. Report completion of this effort to OCIO. Create a POA&M to track progress and verify completion of the action
4	The Deputy Secretary, or his designees, take action to work with OAs to develop internal controls to ensure network administrators are informed and action is taken to disable accounts when users no longer require access.
8	The Deputy Secretary, or his designees, take action to work with FAA to improve their assessment process to meet DOT Cybersecurity Compendium and Security Authorization & Continuous Monitoring Performance Guide. DOT CISO in conjunction with the FAA CIO review the FAA quality assurance process to ensure all security documents are reviewed and updated to reflect the system controls, vulnerabilities, and that the current risks are clearly presented to the Approving Officials.
9	The Deputy Secretary, or his designees, take action to work with the OAs to ensure they update open POA&Ms with the required data fields.
Fiscal Year 2014, OIG Report Number FI-2015-009	
Number	**Recommendation**
5	Start planning and assessing impact of the security requirements that will be affected by NIST SP 800-53 revision 4 and NIST SP 800-53A revision 4.
8	Work with the components to develop a plan to complete annual SAT training within plan milestones. Assess training periodically to determine if the component will meet SAT training plan.
10	Work with the CSMC and individual components (including COE) to develop service level agreements needed to define responsibilities between CSMC and the components. These agreements should include a detailed description of services between parties, at a minimum contain: CSMC and component responsibilities; frequency of periodic scans of DOT networks; access privileges to networks, devices, and monitoring tools; hardware and software asset discovery and on-going management requirements; vulnerability scanning.
12	Work with FAA to revise their plan to effectively transition the remaining 32,266 users to require unprivileged PIV login. Create a POA&M with a planned completion date to monitor and track progress.
16	Work with the Director of DOT Security to develop or revise their plans to effectively transition the remaining facilities to required PIV cards.
Fiscal year 2013, OIG Report Number FI-2014-006	
Number	**Recommendation**
1	Obtain and review specialized training statistics and verify, as part of the compliance

	review process, that all employees with significant security responsibilities have completed the number of training hours required by policy. Report results to management and obtain evidence of corrective actions.
4	Obtain and review plans from FMCSA, MARAD, OST, and RITA to authorize systems with expired accreditations. Perform security reviews of unauthorized systems to determine if the enterprise is exposed to unacceptable risk.
7	Obtain a schedule and action plan for OAs to develop procedures for comprehensive cloud computing agreements to include security controls roles and responsibilities. Report to OA management any delays in completing the procedures.
8	Obtain and review existing cloud computing agreements to assess compliance with agency policy, including security requirements. Report exceptions to OA management.
Fiscal Year 2011, OIG Report Number FI-2012-007	
Number	**Recommendation**
1	Enhance existing policy to address security awareness training for non-computer users, address security costs as part of capital planning, correct the definition of "government system", and address the identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications.
3	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.
Fiscal Year 2010, OIG Report Number FI-2011-022	
Number	**Recommendation**
14	Identify and implement automated tools to better track contractors and training requirements.

Source: OIG.

Exhibit B. Status of Prior Years' Recommendations

EXHIBIT C. DOT'S SYSTEM INVENTORY COUNTS

Table C-1. System Inventory Counts for Fiscal Years 2015 and 2016, by OA

Organization[a]	FY 2015	FY 2016	Change
Federal Aviation Administration (FAA)	318	317	(1)
Federal Highway Administration (FHWA)	19	17	(2)
Federal Motor Carrier Safety Administration (FMCSA)	18	16	(2)
Federal Railroad Administration (FRA)	12	11	(1)
Federal Transit Administration (FTA)	8	8	-
Maritime Administration (MARAD)	17	17	-
National Highway Traffic Safety Administration NHTSA)	16	16	-
Office of Inspector General (OIG)	3	3	-
Office of the Secretary (OST)	43	43	-
Pipeline and Hazardous Materials Safety Administration (PHMSA)	7	7	-
Saint Lawrence Seaway Development Corporation (SLSDC)	1	1	-
Surface Transportation Board (STB)	1	1	-
Total Systems	**463**	**457**	**(6)**

Sources: CSAM as of March 09, 2016 and OIG analysis.

EXHIBIT D. SYSTEMS OVERDUE FOR REAUTHORIZATION

Table D-1. Systems Overdue for Reauthorization, by OA

OA	Asset Reported as Outstanding for Reauthorization	Total
FAA	Access Key Credentialing System[a]	**20**
	Advanced Qualification Program (AQP)	
	Aeronautical Center Security Management System	
	Air Route Surveillance Radar Models 1 & 2[a]	
	Air Transportation Oversight System[a]	
	AML Logistics Center Local Area Network	
	AST Local Area Network[a]	
	Aviation Training Network	
	Building Access, Software And Hardware For MMAC	
	Capability and Architecture Tool Suite (CATS)	
	Certificate Management Information System (CMIS)	
	Computer Based Instruction	
	Customer Service Center System	
	Enterprise Services Center Business Systems	
	Federal Data Registry (FDR)	
	Metasys	
	Mike Monroney Aeronautical Center Voice	
	Office of Airport Local Area Network[a]	
	Radar Training Facility Local Area Network	
	System of Airport Reporting (SOAR)	
FHWA	Central Federal Lands General Support System	**11**
	Correspondence Tracking System	
	Delphi Interface Maintenance System[b]	
	Eastern Federal Lands General Support System	
	Engineer's Estimate Bidding Award Construction System	
	Freedom Of Information Act System	
	National Bridge Inventory System	
	NHI Web Portal and Course Management System	
	Procurement, Requisition Ordering (PRISM)	
	Video Conferencing System	
	Western Federal Lands General Support System	
FMCSA	CoTs DOT LAN[a]	**10**
	Customer Insurance and Registration Information Support (CIRIS)	
	Electronic Document Management System[b]	
	FMCSA LAN Segment at Volpe[b]	
	FMCSA Portal[a]	
	Hazardous Material Package Inspection Program[b]	
	Licensing & Insurance[a]	

OA	Asset Reported as Outstanding for Reauthorization	Total
	Motor Carrier Management Information Systems (MCMIS)[b]	
	National Complaint Hotline Database (NCHDB)	
	SAFETYNET[b]	
FTA	Safety Resource and Training System	**1**
MARAD	BlackBoard[a]	**4**
	Comprehensive Academic Management System[a]	
	Property Management and Archive Record System	
	USMMA LAN[a]	
NHTSA	NHTSA Inventory System[a]	**3**
	PRISM[b]	
	WEB System[a]	
OST	Airline Reporting Data Information System[b]	**21**
	Case Tracking System[a]	
	Civil Rights DBE and Airport Concession Ineligibility Database[b]	
	Confidential Close Call Reporting System[b]	
	Correspondence Control Management System[b]	
	DATMIS (Drug & Alcohol Testing Management Information System)	
	Facilities and Building Management System (FBMS)	
	Grants Notification System (GNS)	
	Image Management System (IMS)	
	Investigative Tracking System[b]	
	Library Systems[b]	
	Prism System	
	RITA Mission Support[b]	
	RITA Web[b]	
	Rulemaking Management System (RMS)	
	Security Operations Systems (SOS)	
	Transtats[b]	
	TSI Infrastructure	
	WEB-enabled Emergency Operations Center (WebEOC)	
	Web Printing System[b]	
	Workman Compensation Information System[b]	
	Total	**70**

[a] Reported in FY 2015 FISMA with an expire Authorization-to-Operate, OA had updated ATO date and provided authorization documentation but it did meet departmental re-authorization requirements.
[b] Reported in FY 2015 FISMA with an expire Authorization-to-Operate, OA have not taken corrective action to re-authorize.
Source: CSAM as of June 11, 2016, and OIG analysis.

Exhibit D. Systems Overdue for Reauthorization

EXHIBIT E. DOT'S CONFIGURATION SETTINGS AND COMMON WEAKNESSES

Table E-1: Configuration Settings and Common Weaknesses, by OA

System Name	Weakness Description	Remediation Status	Planned Finish Date
FAA			
110A (110A Inspector Credentials System)	WebInspect scans are not conducted for IBM Lotus Domino or SharePoint Services-based applications, as these scans tend to produce false-positive results.	Delayed	8/1/2016
AIT EDC (Office of Information and Technology Enterprise Data Centers (EDC))	Due to the consolidation of data centers a complete inventory of assets within the AIF-330 boundary is not available to determine if there is duplicate accounting of information system components in large or complex interconnected systems. Belarc is not deployed on all servers and devices. Therefore, the listing of assets is not complete. In addition, the data centers are unable to provide an accurate listing of what systems the servers are supporting.	Planned/Pending	9/30/2016
	The Assessment Team is not confident that CSMC uses an accurate or complete list of all servers that should be scanned. In addition, patches for third-party software are not automatically applied and AIS 210/AIF 330 lacks a process for tracking, remediating, and reporting weaknesses to management (refer to open POAM 58028)	Delayed	12/31/2015
	Privileged system-level accounts are not reviewed on a regular basis; • A centralized management mechanisms is not in place for Unix and Linux privileged accounts; • Use of privileged accounts is not monitored; • The process for granting Vcenter and KVM privileged access is not defined, documented, monitored, or reviewed.	Planned/Pending	9/30/2016

System Name	Weakness Description	Remediation Status	Planned Finish Date
AOV Facility Specific Safety Standard	The System Owner has not developed change control documentation or established and implemented a process for the AOV FSSS application.	Delayed	9/30/2015
ASTI (Alaskan Satellite Telecommunications Infrastructure)	Baseline testing revealed a number of systems which do not meet the CIS required baseline requirements. In addition, testing identified 5000 missing Redhat Linux patches.	In Progress	9/30/2015
	The SSP does not document under CM-03.e, the retention period for all approved configuration-controlled changes to the system in accordance with the system's Records Disposition schedule.		
ATO Network	CSMC does not scan the AIT Networks GSS on a monthly basis, and the scans that are run do not include all devices within the Networks GSS System boundary.	Planned/Pending	9/1/2016
BMX (Business Management Solutions)	Scans for vulnerabilities were not run against all current web app servers. High vulnerabilities are not entered into the POAM system within the required number of days of detection as outlined in the DOT Departmental Cybersecurity Compendium. BMX does not remediate vulnerabilities within the timeline as outlined in the DOT Departmental Cybersecurity Compendium.	Delayed	6/25/2015
	Patches to correct system vulnerabilities were not applied in accordance with the DOT Cybersecurity Compendium.	Delayed	6/25/2015
CATS (ARP) (Certification Activity Tracking System)	Scan results and assessment results are not reviewed by the system administrator. Critical findings are not corrected as soon as they are discovered. Scan results were not available at the time of this assessment.	Delayed	9/30/2015
CWP (Corporate Work Plan)	MVM and DB protect Vulnerability results were not provided at the time of the assessment. The WebInspect scan results identified Critical and High findings related to Unhandled Exceptions and a BREACH vulnerability in the web application. In addition, ongoing vulnerability scans were not demonstrated.	In Progress	9/30/2015

Exhibit E. Configuration Settings and Common Weaknesses

System Name	Weakness Description	Remediation Status	Planned Finish Date
EASE (Enterprise Architecture & Solutions Environment)	High and Medium vulnerabilities are not remediated within the allotted DOT Compendium timeframe.	Delayed	2/27/2015
FAVES (FAA Administrative Voice Enterprise Services)	Testing discovered many missing patches, some of which are critical.	In Progress	9/16/2016
	There is not a configuration management process in place that would include generating a record of each approved configuration-controlled change.		
	The FAVES system components (Linux, Windows 2008, and Windows 7) are not fully configured and hardened to DOT or USGCB & CIS benchmarks.		
iConect	No vulnerability scans were provided for the web interface or the database, or evidence that vulnerability scans are being conducted on a monthly basis. Not all CIS mandatory configuration settings for all OT products employed on the program are maintained. Not all of the exceptions from the CIS checklists are documented.	Planned/Pending	9/30/2016
ITS (Investigative Tracking System	The FY14 Annual Assessment scanning revealed that all ITS servers are not in compliance with the DOT approved baselines.	Delayed	12/30/2016
	Update: FAA reported completion of this POAM has been pushed out to December of this year.		
	During the FY16 Annual Assessment, scanning revealed that all ITS servers are not in compliance with the DOT approved baselines.	Delayed	12/30/2016
	Update: FAA reported completion of this POAM has been pushed out to December of this year.		
LabNet (William J. Hughes Technical Center Network)	The SSP partially addresses all requirements for control number RA-5.a.1.	Delayed	12/31/2015
LERIS (Labor and Employee Relations Information System)	Database vulnerability scans are not performed on a regular basis.	Delayed	12/31/2015
	The Nessus scans conducted on April 29, 2015 identified 10 Critical, 108 High and 58 Medium vulnerability findings.	Delayed	9/30/2015

Exhibit E. Configuration Settings and Common Weaknesses

System Name	Weakness Description	Remediation Status	Planned Finish Date
Matter Tracking Information System	Software Patch updates not performed on regular basis.	Delayed	9/30/2015
	System is not scanned on a regular basis. Does not meet the FAA testing requirement.	Delayed	9/30/2015
MSAD (Monitor Safety Analyze Data)	Monthly MVM vulnerability scans on MSAD servers are not conducted per the DOT Cybersecurity Compendium	Pending	9/30/2015
	MVM scanning was not completed and the results were not yet available at the completion of the FY15 assessment	Delayed	9/30/2015
PIPS (Payroll Imaging Process Services)	EDC has not remediated the vulnerabilities identified within the DOT established timeframes.	Delayed	3/30/2016
Procurement Automated Tracking System Financials (PATS Financials)	The system's web application did not completely satisfy the requirements of the Security Configuration Baselines Standards based on the order of precedence for configuration benchmarks cited in the DOT Departmental Cyber Security Compendium.	In Progress	9/30/2016
Quality Center Automated Testing (QCAT)	The QCAT operating system platform was successfully scanned using MVM, however the application layer was not scanned for vulnerabilities.	Delayed	7/1/2016
RBRT (Risk Based Resource Targeting)	WebInspect scans are not conducted for IBM Lotus Domino or SharePoint Services-based applications, as these scans tend to produce false-positive results.	Delayed	12/31/2015
	The majority of applications hosted in the EDC (ARB) contain flaws that have been identified during scanning associated with multiple assessments	Delayed	12/31/2015
REMS (Real Estate Management System)	No database or webinspect scans were provided. MVM scans are not conducted or reviewed on a regular basis. This will be addressed as a POA&M item.	Delayed	9/30/2015
	REMS does not scan for vulnerabilities on a regular basis.	Delayed	9/30/2015

System Name	Weakness Description	Remediation Status	Planned Finish Date
SWIM Terminal Data Distribution System	Not all Redhat Security Configuration Benchmarks have been met. Nessus credentialed scan shows many failed compliance checks. An artifact was not provided as part of the FY15 ISCM assessment to validate that this control has been satisfied. Based on examination of the SSP, deviations from checklists were not specifically documented.	In Progress	6/30/2015
	1) A new OpenSSL issue (CVE-14-0224) has been identified for the same assets affected by CVE-14-0160. An OpenSSL issue (CVE-2014-0160) was identified in system assets. Nessus scans revealed Redhat machines are missing many security patches.	In Progress	6/30/2015
VDRP (Voluntary Disclosure Reporting Program)	The MVM scan conducted on April 2, 2015 for VDRP identified high and medium vulnerabilities.	Delayed	9/1/2015
	Scans are not being performed at a defined frequency and vulnerabilities are not being remediated within DOT Policy timeframes.	Delayed	9/1/2015
FRA			
Automated Track Inspection Program (ATIP)	A configuration baseline has not been developed for the ATIP cars.	Delayed	6/21/2013
	Due to resource constraints there is not automation beyond the use of Active Directory for configuration management or monitoring of the system	Not Started	5/3/2016
	Scans are performed only quarterly and web applications are not being periodically scanned.	Not Started	5/3/2016
Railroad Credit Assessment and Portfolio Management System (RCAPM)	RCAPM does not incorporate detection of unauthorized, security-relevant configuration changes. If configuration changes occur, they may be captured on the audit logs that are not monitored or reviewed.	Delayed	2/20/2016
	Currently, the Application server baseline is 68% compliant. The database server baseline is 44% compliant.	Delayed	1/9/2016

System Name	Weakness Description	Remediation Status	Planned Finish Date
FMCSA			
A&I-NCCDB-DataQs	According to the CIS Benchmark scans run on March 14, 2014, this control does not pass for AINEW, AIDB2, AIDBMain, and the CIS Benchmark scan still has to be completed for the IIS Server. The Web Scan run on DataQs on March 5 identified 2 high vulnerabilities. The Web Scan run on A&I on March 3, 2014 identified 1 High vulnerability and 6 Medium vulnerabilities.	Unable to Locate in CSAM	
	The Web Scan run on NCCDB on March 4, 2014 identified 27 high vulnerabilities and 49 medium vulnerabilities		
	"According to the CIS Benchmark scans run on March 14, 2014, this control fails:		
	· AINEW – 91% compliant against Windows Server 2003 Benchmark v3.1.0.1		
	· AIDB2 – 50% compliant against the Windows Server 2008 Benchmark v2.1.0.1		
	· AIDBMain – 78% compliant against Windows Server 2008 R2 Benchmark v2.1.0.1		
FMCSA Service Centers	FMCSA has not fully implemented the relevant security configuration settings FMCSA does not establish or documented or approve any exceptions from the mandatory configuration settings for the Windows 2003/2008 servers as well as the Cisco IOS routers and switches.	Delayed	12/30/2014
MARAD			
Ship Manager Performance Evaluation and Appraisal System (SM PEAS)	Frequency of reviews and updates to the baseline configuration of SM-PEAS is not defined and documented. Circumstances that require reviews and updates to the baseline configuration of SM-PEAS are not defined and documented. Review and updates to the baseline configuration of SM-PEAS are not implemented.	Unable to Locate in CSAM	Unspecified
	Approval of configuration-controlled changes to SM-PEAS with explicit consideration for security impact analysis is not documented.	Unable to Locate in CSAM	

System Name	Weakness Description	Remediation Status	Planned Finish Date
	Approved configuration-controlled changes to SM-PEAS are not documented.		
	Retention and review of records of SM-PEAS configuration-controlled changes are not documented.		
	Frequency with which the SM-PEAS configuration board convenes is not defined in the documentation.		
	Implementation of the configuration board is not documented.		
	Security configuration checklists used by SM-PEAS are not defined. Security configuration checklists are not implemented	Unable to Locate in CSAM	
	Frequency not defined to determine the state of information system components with regard to flaw remediation.	Unable to Locate in CSAM	
	SM-PEAS did not provide documentation for vulnerability scanning tools having the capability to readily update the list of system vulnerabilities scanned.	Unable to Locate in CSAM	
MARAD Internet	The baseline configuration has not been maintained, reviewed, and updated according to the DOT policy.	Not Started	Unspecified
	Frequency of reviews and updates to the baseline configuration of MARAD Internet is not defined and documented in the SSP.		
	Circumstances that require reviews and updates to the baseline configuration of MARAD Internet is not defined and documented in the SSP.		
	Reviews and updates to the baseline configuration of MARAD Internet are not implemented.		
	Older versions of baseline configuration were not documented		
	Approval of configuration-controlled changes to MARAD Internet with explicit consideration for security impact analysis is not documented.	Not Started	Unspecified
	Retention and review of records of MARAD Internet configuration-controlled changes are not documented.		

Exhibit E. Configuration Settings and Common Weaknesses

System Name	Weakness Description	Remediation Status	Planned Finish Date
	Implementation of the configuration board is not documented.		
	Quarterly validation and refresh system images used to deploy systems and virtual machines to update security configuration (*based on current approved benchmarks or baseline standards*) to address new vulnerabilities and attack vectors were not documented.		
	Documentation was not provided showing that the configuration settings are implemented. A baseline configuration for MARAD Internet has not been developed. The website managed by the DOT OCIO that contains the current list of DOT-approved security configuration baselines along with any approved deviations to these baselines was not developed.	Not Started	TBD
	SBCCs that establish mandatory configuration settings for information technology that is used in MARAD Internet were not provided.		
	MARAD Internet does not employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.	Not Started	TBD
	Software patches for MARAD Internet are not tested prior to being installed. MARAD Internet does not use a test environment to conduct patch effectiveness prior to installing patches to the production MARAD Internet servers	Not Started	TBD
Maritime Service Compliance System (MSCS)	MSCS has not defined the frequency of employing automated mechanisms to determine the state of information system components with regard to flaw remediation.	Delayed	Unspecified
	Organizational processes for managing current baseline configuration for MSCS is not in place.	Delayed	Unspecified
	MARAD MCSC does not conduct vulnerability scanning.	Delayed	Unspecified
	There are no configuration settings/Checklists for information technology products employed with in MSCS.	Delayed	Unspecified

Exhibit E. Configuration Settings and Common Weaknesses

System Name	Weakness Description	Remediation Status	Planned Finish Date
	Changes to COE are not tested, validated, and documented prior to implementation.	Unable to Locate in CSAM	
OST			
Investigative Tracking System (ITS)	Web application scans were not performed. Database scans were not performed.	Unable to Locate in CSAM	
Consumer Complaints Application	There is no security configuration guide specifically for the DOT CCA. The CCA system is not scanning to ensure the approved security configuration checklist settings have not been modified. SBCC Scans were requested but not provided. The System Admin indicated no requests for deviations have been submitted for CCA.	Delayed	1/23/2015
	The following scans are not being conducted on the CCA system: • Credentialed Web Application scans (HP Fortify WebInspect) • Credentialed Database Scans (dbProtect) • SBCC scans	Delayed	1/23/2015
Volpe Centralized Data Repository	DOT baselines based on available CIS/DISA standards and recommendations, have not been applied to the components of the VCDR system based upon a review of security configuration baseline reports for both DISA and CIS baseline reviews.	Delayed	11/11/2013
	The VCDR system does not incorporate detection of unauthorized, security-relevant configuration changes into the organization's incident response capability. Configuration policy is scanned but is not performed on a regular basis and the scanning process does not detect configuration changes that may take place	Delayed	10/14/2013

Source: OIG analysis.

EXHIBIT F. PREVIOUS OIG REPORTS IN RESPONSE TO FISMA MANDATES

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

- *DOT Has Major Success in PIV Implementation, but Problems Persist in Other Cybersecurity Areas,* OIG Report Number FI-2016-001, November 05, 2015.
- *DOT Has Made Progress but Significant Weaknesses in its Information Security Remain,* OIG Report Number FI-2015-009, November 14, 2014.
- *DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats,* OIG Report Number FI-2014-006, November 22, 2013.
- *Ongoing Weakness Impede DOT's Progress Toward Effective Information Security*, OIG Report Number FI-2013-014, November 14, 2012.
- *Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information Systems,* OIG Report Number FI-2012-007, November 14, 2011.
- *Timely Actions Needed To Improve DOT's Cybersecurity,* OIG Report Number FI-2011-022, November 15, 2010.
- *Audit of DOT's Information Security Program and Practices,* OIG Report Number FI-2010-023, November 18, 2009.
- *DOT Information Security Program,* OIG Report Number FI-2009-003, October 8, 2008.
- *DOT Information Security Program,* OIG Report Number FI-2008-001, October 10, 2007.
- *DOT Information Security Program,* OIG Report Number FI-2007-002, October 23, 2006.
- *DOT Information Security Program,* OIG Report Number FI-2006-002, October 7, 2005.
- *DOT Information Security Program,* OIG Report Number FI-2005-001, October 1, 2004.

- *DOT Information Security Program*, OIG Report Number FI-2003-086, September 25, 2003.
- *DOT Information Security Program*, OIG Report Number FI-2002-115, September 27, 2002.
- *DOT Information Security Program*, OIG Report Number FI-2001-090, September 7, 2001.

OIG reports are available on our Web site at http://www.oig.dot.gov/.

EXHIBIT G. MAJOR CONTRIBUTORS TO THIS REPORT

Name	Title
Louis King	Assistant Inspector General for Financial and Technology Audits
Michael Marshlick	Project Manager
Martha Morrobel	Senior Information Technology Specialist
Tracy Colligan	Senior Information Technology Specialist
Jenelle Morris	Senior Information Technology Specialist
Jo'Shena Jamison	Information Technology Specialist
Petra Swartzlander	Senior Statistician
Makesi Ormond	Statistician
Susan Neill	Writer-Editor

APPENDIX. AGENCY COMMENTS

Memorandum

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

SUBJECT: **ACTION**: Management Response to the OIG Draft Report— FISMA 2016: DOT Continues to Make Progress But the Department's Information Security Posture is Still Not Effective

DATE: November 3, 2016

FROM: Richard McKinney
DOT Chief Information Officer

RICHARD MCKINNEY
Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=RICHARD MCKINNEY
Date: 2016.11.03 17:41:35 -04'00'

Reply To Attn. of:

TO: Calvin L. Scovel III
Inspector General

Cybersecurity remains among the highest priorities for the Department of Transportation (DOT). We have implemented a Federal Information Security Modernization Act (FISMA) compliant program that tailors the National Institute of Standards and Technology requirements to DOT, with a focus upon investments in people, process, and technology. The Department does not agree with the Office of Inspector General's (OIG) assessment or representation of the Department's cybersecurity program and posture as presented in its annual FISMA audit report. We are committed to investing in, and maturing our cybersecurity program and capabilities, consistent with the mission of DOT and our enterprise shared services strategy. Our progress over the past year includes:

- Executing a network assessment of the Department's Operating Administrations (OAs) and the Chief Information Officer's (CIO) IT Shared Services (ITSS) organization. The Department achieved an 18% improvement in visibility of network infrastructure devices, identified 149 devices for priority replacement, and remediated 72% of 2,385 serious configuration vulnerabilities within 30 days of initial identification;
- Leveraging new capabilities developed during the network assessment, the CIO's ITSS organization remediated 97% of critical vulnerabilities identified by the Department of Homeland Security (DHS) within 45 days of identification;

- Implementing an agency-wide Phishing exercise program, with supplemental training, for all DOT contract and Federal personnel, which achieved a reduction in click-through rates from 55% of 1,250 users in a 2015 exercise to an average 5.44% click-through rate for 68,310 users in 2016 exercises; and
- Deploying and authorizing a new agency personnel security system for 10 of 11 OAs, modeled after solutions in other Federal agencies; implementing Federally-compliant encryption; and leveraging DOT PIV cards for strong authentication to the system.

In addition, DOT is investing in other areas to strengthen the Department's cybersecurity program. For example, we are collaborating with DOT's Office of Human Resources, the Office of Management and Budget (OMB), and the Office of Personnel Management (OPM), and other agencies on the Federal cybersecurity workforce initiative to strengthen the Federal cyber workforce, streamline recruiting, and improve the retention of skilled personnel. Further, we are partnering with other DOT organizations to integrate cybersecurity into DOT's safety management programs.

Upon review of the draft report, we agree with recommendations 1-4, and 6, as written. We do not concur with recommendation 5 as neither Federal nor DOT policy require disaggregation of an identified weakness into a Plan of Action and Milestones (POAM) for each related control, and doing so introduces unnecessary complexity and inefficiencies into weakness management. We also do not concur with recommendation 7 as written, and instead propose to reinforce system owner responsibilities through additional guidance regarding documentation and implementation of controls for systems. Lastly, we do not concur with recommendation 8, as neither Federal nor DOT policy requires tracking of discrete technical vulnerabilities as individual POAMs and doing so would be highly inefficient and burdensome. Instead, we propose to address the OIG's findings by focusing on the effectiveness of OA's vulnerability management programs and any associated control-level weaknesses.

We will provide you proposed corrective actions and milestones for each recommendation within 60-days of the Final report's issuance. We appreciate the opportunity to comment on OIG's draft report. If you have any questions, please contact me at 202-366-9201.