U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

FISMA 2017: DOT's Information Security Posture Is Still Not Effective

OST

Report No. FI2018017

January 24, 2018

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

FISMA 2017: DOT's Information Security Posture Is Still Not Effective

Required by the Federal Information Security and Management Act of 2002

Office of the Secretary of Transportation | FI2018017 | January 24, 2018

What We Looked At

The Federal Information Security Management Act of 2002 (FISMA), as amended, requires inspectors general to conduct annual reviews of their agencies' information security programs and report the review results to the Office of Management and Budget (OMB). DOT's operations rely on 464 information technology systems, which represent an annual investment of approximately $3.5 billion. Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

In all five function areas, we found DOT to be at the Defined maturity level—the second lowest tier of the maturity model for information security—because the Department has, for the most part, formalized and documented its policies, procedures, and strategies. However, these policies and procedures are not consistently implemented throughout DOT.

Identify controls include risk management, weakness remediation, and security authorization. Protect controls include configuration management, identity and access management, and security training. Detect controls are used to identify cybersecurity incidents as part of information security continuous monitoring (ISCM). Respond controls cover incident handling and reporting. Recover controls cover development and implementation of plans to restore capabilities and services impaired by cybersecurity incidents. DOT's Identify, Protect, Detect, Respond, and Recover controls are currently inadequate.

Our Recommendations

We made eight recommendations to help the Department address the challenges in developing a mature and effective information security program. DOT concurs with six of our recommendations, partially concurs with one, and non-concurs with one.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: January 24, 2018

Subject: ACTION: FISMA 2017 DOT's Information Security Posture Is Still Not Effective | Report No. FI2018017

From: Louis C. King
Assistant Inspector General for Financial and Information Technology Audits

To: Chief Information Officer

The Department of Transportation's (DOT) operations rely on 464 information technology (IT) systems, 323 (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 support transportation-related operations including air traffic control and pilot licensing. Others support inspection and oversight for highway safety and hazardous material transport.

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 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 OMB.

[1] Pub. L. No. 107-347 (2002); 44 U.S.C. Chapter 35, Sub Chapter II, Information Security.
[2] The Federal Information Security Modernization Act of 2014 (Pub. L. 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.

For this fiscal year's review, OMB required inspectors general to assess 54 metrics in 5 security function areas to determine information overall security program maturity[3] at 1 of 5 levels defined by OMB. These levels are—from lowest to highest—Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. OMB defines effectiveness as being Managed and Measurable in all function areas.

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 ending June 30, 2017. Specifically, we assessed DOT's performance in five function areas—Identify, Protect, Detect, Respond, and Recover.[4]

We conducted our work in accordance with generally accepted Government auditing standards. To address OMB's 2017 FISMA reporting metrics, we assessed 45 sample systems, interviewed Department officials, and analyzed data in DOT's Cybersecurity Assessment and Management System (CSAM)—a repository the Department uses to track system inventories, weaknesses, and other security information. See exhibit A for more details on our scope and methodology. As required, we provided our results to OMB via its web portal.[5] Exhibit B lists the entities we visited or contacted.

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

cc: The Secretary
DOT Audit Liaison, M-1

[3] OMB's *FY 2017 Inspector General FISMA Act of 2014 Reporting Metrics* (2017) prescribes the metrics and provides a new methodology to assess the maturity of a program's function area.
[4] OMB's function areas align to the National Institutes of Standards and Technology's (NIST) *Framework for Improving Physical Infrastructure Security* (2014).
[5] Because OMB designates this information For Official Use Only, our submission to OMB is not contained in this report.

Results in Brief

The Department's cybersecurity program remains ineffective based on OMB's methodology.

In all five function areas, we assessed DOT at the Defined maturity level because the Department has, for the most part, formalized and documented its policies, procedures, and strategies. However, these policies and procedures are not consistently implemented throughout DOT. We found progress from last year's overall Ad Hoc maturity level, but DOT's information systems remain vulnerable to serious security threats due to the deficiencies in the function areas as follows:

1. Identify. DOT's Identify controls, which include risk management, weakness remediation, and security authorization, are inadequate. While the Department has policies and procedures for a risk management program, they are not consistently implemented. For example, four Operating Administrations (OA) did not adhere to the Department's guidance to develop and disseminate risk management policies and procedures for its programs. Additionally, we found DOT operated 71 systems with expired authorizations to operate. 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) OCIO does not sufficiently oversee the remediation and closure of plans of action and milestones6 (POA&M) for system weaknesses; and (4) FAA's and other OAs' management of contractor operated systems did not always comply with requirements. Based on OMB metrics, DOT's Identify controls are at the Defined level of maturity.

2. Protect. DOT's Protect controls, which include configuration management, identity and access management, and security training, are not adequate. For example, we found 123 configuration-related weaknesses in 40 of 45 sample systems that were either not documented in CSAM or have passed or are approaching planned finish dates for remediation. Additionally, the Department has not transitioned all of its information systems to use of multifactor user identity authentication. For example, only 125 of 453 systems reported in CSAM required personal identity verification (PIV) cards for user identity and authentication. The Department also has not fully implemented the use of PIV cards for physical access to facilities

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

where required by Federal policy. FAA informed us it had enabled 155 of 516 facilities for PIV access. The Department will not complete this implementation for its remaining facilities until fiscal year 2018. Lastly, the Department did not provide adequate support to demonstrate that appropriate security staff had received necessary specialized training. Based on OMB metrics, DOT's Protect controls are at the Defined level of maturity.

3. Detect. DOT's Detect controls, which are used to identify cybersecurity incidents as part of information security continuous monitoring (ISCM),[7] are not adequate. The Department lacks complete inventories of hardware and software, and fully automated and integrated configuration setting management and common vulnerability management. For example, OCIO's most recent quarterly report to OMB did not match the OAs individual inventories. According to DOT's Chief Information Security Officer, a serious failure in OCIO's continuous monitoring software tool occurred late in 2016, and as a result, OAs had difficulty using the application for FISMA reporting and asset management. OCIO also has not provided the OAs with clear guidance on what data they must provide to OCIO, or a process for developing and maintaining an up-to-date inventory of software assets used in the Department with the detailed information for tracking and reporting. Based on OMB metrics, DOT's Detect controls are at the Defined level of maturity.

4. Respond. DOT's Respond controls, which cover incident handling and reporting, are insufficient. The Department has yet to address recommendations we made to resolve issues that we found with the Department's Cyber Security Management Center's (CSMC) which handles cybersecurity incidents. CSMC lacks access to all departmental systems and network maps, as well as a ranking scheme to address incidents based on the seriousness of the risk they pose. We also found that the OAs do not comply with all FISMA and DOT requirements regarding incident response. Specifically, we found 17 security incident-related weaknesses in 16 of 45 sample systems that have not been remediated as scheduled. As a result of its inability to monitor all DOT systems, CSMC cannot report all incidents to the United States Computer Emergency Readiness Team (US-CERT) at DHS. Consequently, DOT and US-CERT cannot be sure that they are mitigating cyber incidents effectively. Based on OMB metrics, DOT's Respond controls are at the Defined level of maturity.

[7] 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.

5. Recover. DOT's Recover controls—for developing and implementing plans to restore capabilities and services impaired by cybersecurity incidents—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 a service disruption. Among our 45 sample systems, we found that 10 OAs had deficiencies in their contingency plans and testing for at least 1 system. We also found that 23 sample systems did not meet OMB and FISMA requirements for contingency planning and testing. Based on our sample of 45 systems, we estimate that for 319 of 4598 systems, or 69.4 percent, the OAs did not perform effective contingency planning or testing. Based on OMB metrics, DOT's Recover controls are at the Defined level of maturity.

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

Background

Under FISMA, 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. Furthermore, OMB regulations[9] require 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, and the Government Accountability Office (GAO) on the adequacy and effectiveness of its information security policies, procedures, and practices.

DOT's 11 OAs[10] manage the Department's 464 information systems. 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. DOT's cyber security program is critical to protect

[8] Our 459 estimate has a precision of +/-59 systems at the 90-percent confidence level.
[9] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (2016).
[10] In prior years, we reviewed 12 OAs. However, as a result of the STB Reauthorization Act of 2015, the Surface Transportation Board (STB) is no longer part of DOT. For purposes of this report, OST and OIG are treated as OAs. See exhibit C for a list of the 11 OAs.

these systems from malicious attacks or other compromises that may inhibit its ability to carry out its functions and missions.

For this year's review, OMB and DHS, in consultation with the Council of the Inspectors General on Integrity and Efficiency and the Federal Chief Information Officer Council, revised the metrics[11] for inspectors general reviews. These metrics are organized around the five security functions—Identify, Protect, Detect, Respond, and Recover—outlined in NIST's cybersecurity framework. See table 1 for definitions of these functions and the number of metrics in each function.

Table 1. Cybersecurity Framework Functions and Definitions

Cybersecurity Framework Function	Definition	No. of metrics for FISMA 2017
Identify	Requires agencies to develop the understanding needed to manage security risks to systems, assets, data, and capabilities. Includes metrics for risk management, weakness remediation, and security authorization.	12
Protect	Requires agencies to develop and implement appropriate safeguards to ensure delivery of infrastructure services. Includes metrics for configuration management, user identity and access management, and security training.	23
Detect	Requires agencies to develop and implement processes to identify incidents that may include security breaches. Includes metrics for information security continuous monitoring.	5
Respond	Requires agencies to develop and implement processes for remediating detected cybersecurity incidents. Includes metrics for incident response.	7
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. Includes metrics for contingency planning.	7

Source: OMB and DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (2017).

In the guidance, OMB and DHS define 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.

[11] OMB and DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (2017).

Table 2. Cybersecurity Maturity Levels and Definitions

Maturity Level (from lowest to highest)	Definition
Ad Hoc	Policies, procedures, and strategy are not formalized; activities are performed in a reactive manner.
Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Consistently Implemented	Policies, procedures and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable	Quantitative and qualitative measures are collected across the organization, and used to assess the effectiveness of policies, procedures, and strategy and make necessary changes.
Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: OMB and DHS, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (2017).

CSAM is DOT's departmentwide system inventory and weakness repository and monitoring system. It facilitates DOT's identification of threats and vulnerabilities and provides comprehensive IT weakness tracking and reporting.

Since 2001, we have published 16 reports that present the results of our evaluations of DOT's information security program and practices in accordance with FISMA requirements. See exhibit H for a list of our previous reports.

Identify: DOT's Identify Function Controls Are Inadequate

DOT's Identify controls—which include risk management, weakness remediation, security authorization and controls over contractor-operated systems—are not adequate. The Department has defined policies and procedures for risk management, but has not sufficiently implemented them. Furthermore, some OAs' management of contractor-operated systems are not fully compliant and those with cloud systems have not executed agreements with their cloud services providers that cover system security.

The Department Has Not Fully Implemented Risk Management

Not all of DOT's OAs have implemented risk management programs according to requirements. The Department has policy and procedures[12] for risk management that, for the most part, define the risk management program. These policies and procedures require the OAs to develop and implement their own programs, but not all OAs have done so. Several OAs have also not developed other aspects of risk management—information sharing on threats, timely system reauthorization, monitoring of common controls, and weakness remediation.

Four OAs Have Not Fully Developed Risk Management Programs

DOT has policies and procedures for risk management, but not all 11 OAs have fully implemented it. DOT's Cybersecurity Compendium states that each OA must develop, disseminate, review, and annually update risk management policy and procedures. FAA, FHWA, FMCSA, FRA, FTA, OIG, and PHMSA have policies and procedures for their risk management programs that include appropriate elements such as criteria for making risk based decisions. The remaining OAs—MARAD, NHTSA, OST, SLSDC—did not provide copies of their risk management policies and procedures.

- MARAD's Security Official informed us that their organization's standards and procedures are in draft form.
- NHTSA's Security Official informed us that NHTSA plans to develop a risk management standard operating procedure that follows DOT's plan and processes.
- OST's Security Officials informed us that OST adheres to DOT's Security Authorization and Continuous Monitoring Guide and DOT's Weakness Management Guide in its risk management strategy.
- SLSDC's Security Official stated that the Agency's risk management program remains at an ad-hoc level of maturity.

[12] DOT Order 1351.37, Departmental Cybersecurity Policy (2011); DOT, *Security Authorization and Continuous Monitoring Performance Guide, ISCM Strategy, Risk Management, and Continuous Monitoring Program* (2016); *Department Cybersecurity Compendium, Supplement to DOT Order 1351.37 DOT Cybersecurity Policy* (2015).

The Department Has Not Established Information Sharing on Threat Activity

The Department has not established information sharing on threat activity. We did not receive sufficient documentation to determine whether DOT's senior officials are regularly briefed on threat activity. OMB requires[13] agencies to establish and promote transparency by communicating information about potential risk. We received documentation on vulnerability remediation dated February and March 2017 but none for the months of April through June 2017. OCIO officials informed us that they shared information on threat activity with the OAs through several mechanisms, including briefings to the CIO on vulnerabilities and threats and cybersecurity performance and risks, and e-mails from the Chief Information Security Officer on new vulnerabilities, phishing attacks, and other threats.

A lack of effective communication on cybersecurity threats throughout the Department can leave OAs' information systems vulnerable to compromise.

The Department Operates Systems With Expired Authorizations

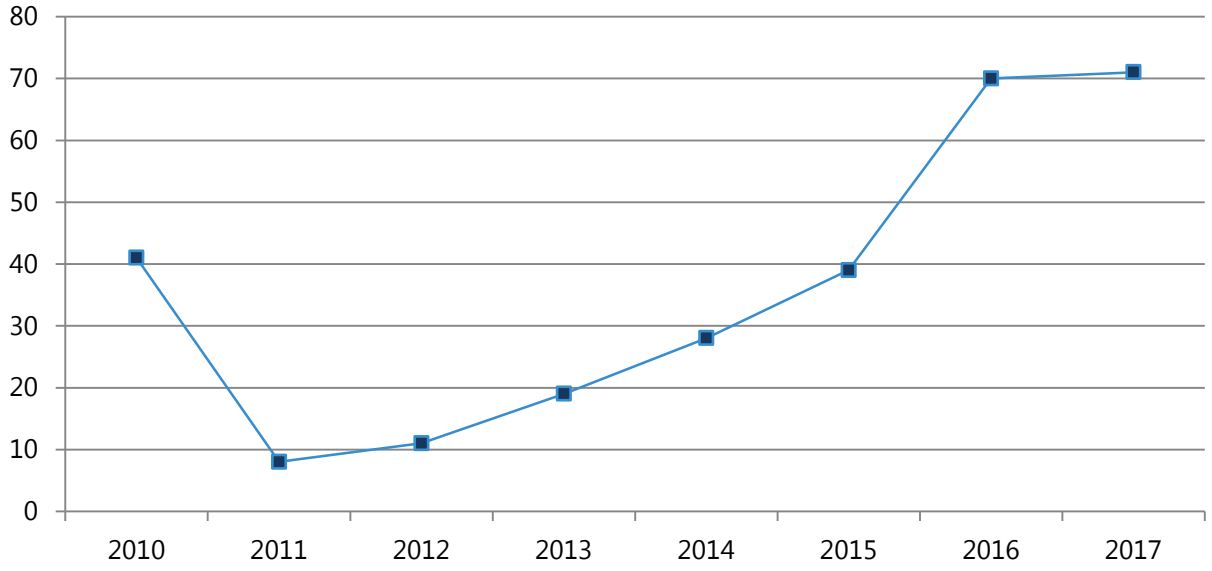
As in previous years, DOT operates systems that have expired authorizations. OMB requires[14] each Federal agency to test at least annually and authorize at least once every 3 years the operation of each system. A senior agency official must authorize or reauthorize each system when he or she has determined that the system's operation poses an acceptable level of risk. Furthermore, the Department's guidelines on security authorization and continuous monitoring performance[15] requires that the tasks associated with planning, implementing, assessing, managing and monitoring information security and the associated risk to the information system must be performed.

Among the universe of 464 departmental systems, we found 71 systems that had expired authorizations to operate, while in 2016, we found 70 systems were unauthorized. See figure 1 for information on unauthorized systems since 2010.

---

[13] OMB Memorandum M-16-17; OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (2016).
[14] OMB Circular A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources* (2016); OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* (2016).
[15] DOT, *Security Authorization and Continuous Monitoring Performance Guide, ISCM Strategy, Risk Management, and Continuous Monitoring Program* (2016).

Figure 1. Numbers of Systems With Expired Authorizations To Operate Since 2010



Source: CSAM and OIG analysis.

These 71 systems[16] belong to 8 OAs (see table 3). We found that these OAs' information security system managers have not provided their authorizing officials with sufficient information to make decisions for reauthorization.

[16] See table D-1 in exhibit D for a list of these 71 systems.

Table 3. Systems Overdue for Reauthorization as of June 2017, by OA

OA	Number of Systems
FAA	33
FHWA	5
FMCSA	10
FTA	1
MARAD	5
NHTSA	4
OST	12
PHMSA	1
Total	71

Source: CSAM and OIG analysis.

Furthermore, for 35 of our 45 sample systems, the OAs authorized system operation without adequate supporting documentation. We also found 23 sample systems that had inadequate or no evidence of current security control assessments, and 33 sample systems whose system owners did not effectively monitor their systems' security controls (continuous monitoring). See table 4 for these systems by OA. Based on our sample of 45 systems, we estimate that:

- 369 of 459 systems, or 80.4 percent,[17] were operating with authorizations that were not fully supported.
- 271 of 459 systems, or 59.1 percent,[18] were operating without adequate security control assessments.
- 350 of 459 systems, or 76.3 percent,[19] were operating without continuous monitoring.

This lack of on-going security monitoring, assessments, and system re-authorization makes it difficult for authorizing officials to responsibility make effective decisions that operating systems do not represent unwarranted risks to the Federal Government.

[17] Our 80.4 percent estimate has a margin of error of +/-11.0 percentage points at the 90 percent confidence level.
[18] Our 59.1 percent estimate has a margin of error of +/-14.2 percentage points at the 90 percent confidence level.
[19] Our 76.3 percent estimate has a margin of error of +/-12.2 percentage points at the 90 percent confidence level.

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

OA	Systems Tested	Inadequate Authorization to Operate	Inadequate Security Control Assessments	Inadequate Continuous Monitoring
FAA	23	19	15	18
FHWA	3	2	1	2
FMCSA	2	2	1	2
FRA	2	2	0	1
FTA	2	1	0	1
MARAD	2	2	2	2
NHTSA	2	1	1	1
OIG	2	2	2	2
OST	5	3	1	3
PHMSA	2	1	0	1
SLSDC*	0	0	0	0
Total	**45**	**35**	**23**	**33**

* SLSDC was not selected as part of the sample systems.
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. OMB requires[20] common control providers[21] to do the following:

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.

[20] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information System* (2013).
[21] The entity that has a system control used by another system.

As in previous years, DOT's policy and procedures for common controls—which do not cover FAA's common controls—lack practices for monitoring and authorizing controls. We found the following issues with the common controls provided by OST's common operating environment (COE),[22] OIG, and FAA:

- Supporting documentation on the controls' continual assessments was insufficient;
- Security officials had not completed reauthorization assessments for the controls;
- Personnel had not finalized guidance for customer agencies' use of the controls;
- Regular communication between authorizing officials and common control providers had not been established regarding the controls' security status and inherited risk.[23]

This lack of comprehensive procedures and effective oversight of common controls could result in security incidents that go undetected.

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

Federal agencies must comply with several requirements in their remediation of known security weaknesses. FISMA requires agencies to develop processes to remediate security weaknesses that they detect during system monitoring and testing. OMB[24] requires agencies to develop POA&Ms for these weaknesses and to prioritize weakness remediation based on the seriousness of each weakness. Furthermore, DOT policy[25] requires OAs to categorize their systems' weaknesses as low, medium, or high priorities based on their own criteria, and to record all weaknesses and POA&Ms in CSAM. Untracked and unresolved POA&Ms make it difficult for DOT to be sure that its systems are secured and protected.

We found that the Department has 4529 open POA&Ms—a reduction of 391 (.08 percent) from 2016's 4920—some of which date from 2009 (see table 5). We noted the following deficiencies in these POA&Ms:

[22] A network managed by OST that provides centralized IT services, including email management, computer infrastructure, internet access, and other services to users (FAA does not use COE's services).
[23] Risks associated with security controls or portions of security controls controlled by another organization (either internal to DOT or external).
[24] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (2001).
[25] DOT Order 1351.37; DOT, *Security Weakness Management Guide* (2017).

- 1360 POA&Ms, including 296 high priority and 1064 medium priority, had start dates for remediation marked "to be determined," indicating that the OAs had not begun work to resolve the weaknesses;
- 737, including 170 high priority and 567 medium priority, did not document remediation costs.

Table 5. Summary of POA&Ms Opened Between 2009 and 2017 Without Start Dates or Documented Remediation Costs, by OA

OA	Total Open POA&Ms	Actual Start Date marked as "TBD"	No Documented Cost
FAA	2625	815	243
FHWA	23	0	0
FMCSA	529	72	72
FRA	106	68	0
FTA	73	0	0
MARAD	445	132	123
NHTSA	41	23	9
OIG	7	1	1
OST	599	196	267
PHMSA	81	53	22
SLSDC	0	0	0
Total	**4529**	**1360**	**737**

Source: CSAM POA&M report dated August 31, 2017.

Furthermore, the information on POA&Ms in CSAM for our sample systems was not complete. We found the following:

- For 33 of 45 sample systems, the OAs had not submitted POA&Ms on all identified security weaknesses to CSAM. Based on our sample of 45 systems, we estimate that 369 of 459 systems, or 80.4 percent,[26] have system specific security weaknesses that are not reported and managed in CSAM.

[26] Our 80.4 percent estimate has a margin of error of +/-11.0 percentage points at the 90 percent confidence level.

- FAA had not established POA&Ms for weaknesses identified in 185 audit recommendations on its air traffic control information security program that GAO made in a 2015 report.[27] As of September 8, 2017, FAA had closed 34 of these recommendations. A representative of the Department's Chief Information Security Officer informed us that the OAs are tracking GAO's recommendations in accordance with DOT and Federal policies.[28] However, we did not find any of GAO's recommendations to the OAs reported in CSAM.

- As of July 28, 2017, OCIO had not reported POA&Ms to CSAM for 24 open recommendations from our previous FISMA reports.

- As reported last year, FAA reports to CSAM multiple weaknesses as a single weakness.

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

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

Some OAs' management of their contractor-operated systems did not comply with all requirements. Contractor-operated systems, including cloud systems, are either fully or partially owned or operated by a contractor, or another agency or entity. Contractor systems present unique risks because the Department frequently does not manage their security controls.

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

OMB requires[29] 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.

---

[27] GAO, *Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems* (GAO-15-221), January 2015.
[28] OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones* (2001); OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (2004).
[29] OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (2010).

We found that FAA has 134 contractor systems that it has miscategorized as Agency-operated systems, including 122 we identified in our 2016 review. According to FAA officials, these 134 systems should not be classified as contractor systems. FAA officials also informed us that the Agency is developing guidance with criteria and a methodology for identifying contractor owned and operated systems that will help establish consistent identification of contractor systems. FAA anticipates completing this guidance by September 30, 2019.

OCIO stated that it does not have detailed visibility, management control, or oversight authorities over FAA. The lack of accurate information on who operates, and maintain the Department's systems makes it difficult for DOT to provide direction to the OAs and contractors on information security, to enforce compliance with information security requirements, and to ensure security risks are reduced.

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

OAs have not executed agreements with cloud services providers that cover security for their cloud systems. Cloud computing provides convenient access to computing resources, including networks, servers, storage, and applications. Cloud computing services 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 cloud computing security requirements for Federal agencies, documented in OMB's Federal Risk and Authorization Management Program (FedRAMP). OMB's guidelines[30] help agencies satisfy FedRAMP's requirements with standard language for contracts and service agreements with providers. One FedRAMP requirement calls for each OA to execute an agreement with each 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 the COE cloud computing services did not provide evidence that they have complied with FedRAMP's requirement to execute agreements that clearly specify responsibilities for cloud system security. The lack of these agreements makes it difficult for the Department to ensure that service providers effectively manage the security of DOT's data in cloud systems.

[30] OMB Circular A-130, *Managing Information as a Strategic Resource* (2016).

Protect: DOT's Protect Function Controls Are Not Adequate

DOT's Protect controls—which cover configuration management, user identity and access management, and security training—are inadequate. Furthermore, some OAs did not meet some security training requirements outlined in DOT's defined security training program.

DOT's Controls Over Configuration Management Are Inadequate

We found that OCIO does not enforce compliance with OMB's requirements[31] for 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

During our review, we found 123 configuration-related weaknesses in 40 of 45 sample systems, and 10 of 12 common control providers[32] that were either not documented in CSAM or have passed or are approaching planned finish dates for remediation. For example, we found various instances where OAs did not have

[31] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (2013).
[32] Organizations implementing common controls are referred to as common control providers. Common controls are security controls whose implementation results in a security capability that is inheritable by multiple systems. For example, systems hosted in a data center will typically inherit controls that provide physical, environmental, and network protection.

adequate mechanisms or controls to disable inactive accounts. See exhibit E for weaknesses in configuration management.

Unremediated system weaknesses expose the Department's networks and information systems to compromise that could result in loss, damage, and misuse of data and other valuable assets

DOT's Controls Over User Identity and Access Management Are Inadequate

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 by at least two unique factors. DOT policy[33] requires that PIV cards must be the primary means of identification and authentication for access to its information systems. OMB also requires[34] agencies to implement the use of PIV cards for access to departmental facilities by both employees and contractors.

We found that the Department has not transitioned all of its information systems to use of multifactor user identity authentication. As of October 6, 2017, 125 of 453 systems[35] reported in CSAM required PIV cards for user identity authentication. However, as in previous years, we found that the Department does not ensure that OAs comply with this requirement. Specifically, we found the following:

- 220 systems that were not enabled for PIV card use, and 38 that were unspecified, or it was not indicated whether the system could use PIV cards);
- 70 systems were enabled for PIV access but the systems did not require users to use PIV, which permits users to employ less secure means for authentication such as usernames and password;
- 51 of 166 operational systems containing PII that did not use PIV cards for authentication;

[33] DOT Cybersecurity Compendium.
[34] OMB Memorandum M-11-11, *Policy for a Common Identification Standard for Federal Employees and Contractors* (2011).
[35] FAA officials stated that National Air Space systems are exempted from user identity authentication with PIV cards, and the Agency plans to develop a waiver for this exemption by December 29, 2017.

- In 28 of 45 sample systems, and for 8 of 12 common control providers, we found 39 weaknesses in user identity and access management (see exhibit F) that were either not documented in CSAM or had passed or were approaching planned finish dates for remediation.

Finally, as in prior years, the Department has not fully implemented the use of PIV cards for physical access to facilities where required by Federal policy. FAA informed us that as of September 22, 2017, it had enabled 155 of 516 facilities for PIV card access. FAA officials also informed us that the Agency has developed plans to implement PIV card access at its high risk facilities[36] and implementation at the remaining facilities by the end of fiscal year 2018.

In 2016, we found that DOT was deploying Virtual Desktop Infrastructure (VDI)[37] without the required use of PIV cards for access. Department officials informed us that technical and financial challenges delayed full implementation of mandatory use of PIV cards for VDI access, and that the Department planned to resolve the issues by December 2016. However, this weakness has not been remediated.

The lack of required user identity authentication and access controls may lead to unauthorized access to DOT's information systems. Furthermore, the lack of PIV card use 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.

Some OAs Did Not Meet All 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 can access agency information systems. Furthermore, both FISMA and OMB require[38] agencies to provide security awareness training to all employees and contractors, even those that never access computer systems.

[36] FAA rates each facility with a level of risk for compromise. Low risk facilities generally have moderate levels of contact with the public with activities that are routine in nature. Medium risk facilities generally have 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. High risk facilities generally have 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.

[37] VDI enables a user to have a DOT server replicate his or her desktop on devices in addition to a Government-issued computer.

[38] OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (2007).

The Department required,[39] that by September 15, 2017, the OAs ensure that 95 percent of their personnel completed security awareness training. FHWA, FRA, FTA, NHTSA, OIG, PHMSA and SLSDC exceeded this goal and FRA and OIG achieved 100 percent (see table 6). Overall, 90 percent of Department personnel completed training. However, MARAD did not meet the goal and provided documentation that included outdated training completion dates covering 2007 and 2016 for some personnel.

Table 6. Percentage of Security Awareness Training (SAT) Completed, by OA, as of September 15, 2017

OA	Completed	Not Completed	Total Employees Requiring SAT	% Completed
FAA	53,736	5218	58,954	91%
FHWA	3164	60	3224	98%
FMCSA	1380	122	1502	92%
FRA	1255	1	1256	100%
FTA	731	5	736	99%
MARAD	765	149	914	84%
NHTSA	907	22	929	98%
OIG	378	0	378	100%
OST[a]	1885	403	2288	82%
PHMSA	737	10	747	99%
SLSDC	129	1	130	99%

[a] Includes Volpe.
Source: OIG analysis.

Furthermore, DOT's cybersecurity policy—characteristic of a program at a defined level of maturity—requires OAs to provide specialized training for personnel that perform certain security related roles. These personnel must complete training courses on specialization areas in the National Cybersecurity Workforce

[39] DOT, CAM-2017-001, *FY17 Mandatory Security Awareness Training Implementation Guidance* (2017).

Framework[40] developed by the National Initiative for Cybersecurity Education. The Framework lists and defines 33 specialization areas in cybersecurity and identifies common tasks and knowledge, skills, and abilities associated with each area. OCIO's guidance[41] 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 the following issues with the OAs' specialized training:

- MARAD provided information on personnel's specialized training that occurred in fiscal year 2016.
- Personnel at FAA, MARAD, NHTSA, OIG, OST and SLSDC did not complete specialized training requirements by the September 15, 2017 deadline.
- FTA provided information on its specialized training but not on how personnel's roles related to the Framework's specialized areas or which competencies each training course covered.

Lack of regular security awareness training could result in behaviors that put DOT's information at risk, such as incorrect user ID and password development, and internet misuse. Furthermore, the lack of specialized training for personnel 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's Detect controls—which cover information security continuous monitoring—are not adequate. DOT lacks a complete inventory of its hardware and software. In addition, as previously discussed, we found weaknesses with CSM and CVM. Although not fully functional or properly implemented, these controls are at the defined level of maturity because DOT has, to a large extent, formalized its policies, and procedures.

As in 2016, we found that the Department's inventories of both its hardware and software assets were incomplete. NIST standards[42] and DOT's security policy

[40] NIST SP 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (2017).
[41] DOT, CAM-2017-002, *FY17 Specialized Cybersecurity Training Implementation Guidance* (2016).
[42] NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (2011).

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[43] to OMB did not match the OAs' individual inventories. The OAs had difficulty using the Department's application for continuous monitoring—the CDM/BigFix[44]—because, according to DOT's Chief Information Security Officer a serious failure of the application's infrastructure occurred in 2016. OST informed us that BigFix was still being reconfigured. OCIO did not provide a hardware inventory for the Department. Seven modes—FAA, FHWA, FMCSA, FRA, FTA, NHTSA, OST, and PHMSA—provided inventory listings for a total of 127,617 hardware assets. These inventories also included workstations and servers but not other devices such as routers.

Furthermore, OCIO has not provided the OAs with clear guidance on what data they must provide to OCIO or a process for developing and maintaining an up-to-date inventory of software assets with the detailed information for tracking and reporting. For example, while OCIO's guidance[45] discusses asset discovery and management, it does not provide information on how to track and report this information. Furthermore, OAs that use the BigFix could not provide software asset inventories because of the tool's failure. Furthermore, OCIO has not set a frequency for the OAs to report to it on their assets. As a result, some OAs report quarterly while others report annually.

This lack of a 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.

[43] Chief Information Officer 2017 Quarter 3 FISMA Report.
[44] The CDM/Big Fix identifies cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first.
[45] DOT, *Security Authorization and Continuous Monitoring Performance, ISCM Strategy, Risk Management, and Continuous Monitoring Program* (2016).

Respond: DOT's Respond Controls Are Not Sufficient

DOT's Respond controls, which address incident response, are insufficient. According to DOT policy,[46] when an incident such as a security breach or interruption of service occurs, the OA must report the incident to CSMC. CSMC analyzes the incident, categorizes it, and reports it to US-CERT at DHS. DOT's 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. Based on OMB's 2017 FISMA metrics, we determined that DOT's Respond function is at the Defined maturity level. Although the Department has established policies, procedures, and processes governing incident response—characteristic of a program at a defined level of maturity—we found that specific controls are not consistently implemented.

During our 2016 audit of DOT's cybersecurity incident handling, we found that CSMC did not have access to all departmental systems to monitor them for security incidents or a ranking scheme to address incidents based on the seriousness of the risk they pose. Currently, all four recommendations in our report[47] are open. OCIO informed us of the Department's intended actions to respond to the recommendations, but as of October 1, 2017, we have not received follow-up communication.

During this year's FISMA review, we found that the OAs do not comply with all FISMA and DOT requirements regarding incident response. Specifically, we found 17 security incident-related weaknesses in 16 of 45 sample systems and 6 of 12 common control providers that have not been remediated as scheduled (see exhibit G).

As a result of its inability to monitor all DOT systems, CSMC cannot report all incidents to US-CERT. Consequently, DOT and US-CERT cannot be sure that they are mitigating cyber incidents effectively. Furthermore, incidents not reported to US-CERT inhibit DHS's ability to ensure that Federal systems and information are secure from compromise.

[46] OCIO, *Cyber Security Incident Response Plan* (2014).
[47] *DOT Cybersecurity Incident Handling and Reporting Is Ineffective and Incomplete* (OIG Report Number IF2017001), October 2016.

Recover: DOT's Recover Function Controls Are Not Consistently Implemented

DOT's Recover controls for contingency planning are not implemented at all 11 OAs, but is at a Defined level of maturity because DOT has, for the most part, formalized policy and procedures for this function. DOT policies[48] require agencies to establish and periodically test contingency plans[49] 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.

Among our 45 sample systems, we found that 10 of the 11 OAs[50] were not implementing DOT's contingency plans and testing requirements for at least 1 system. We also found that 23 sample systems did not meet OMB and FISMA requirements for contingency planning and testing. Based on our sample of 45 systems, we estimate that for 319 of 459 systems, or 69.4 percent, the OAs did not perform effective contingency planning or testing.[51] See table 7 for a summary of these deficiencies.

[48] DOT Cybersecurity Compendium.
[49] 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 or disaster recovery plan for major disruptions. A disaster recovery plan details the recovery of one or more information systems at an alternative facility in response to a major hardware or software failures 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.
[50] SLSDC did not have a sample system selected for this year's FISMA review.
[51] Our 69.4 percent estimate has a margin of error of +/- 12.9 percentage points at the 90 percent confidence.

Table 7. Summary of Deficiencies in Contingency Planning and Testing for Sample Systems, by OA

Contingency Planning and Testing Requirements*	FAA	FHWA	FMCSA	FRA	FTA	MARAD	NHTSA	OIG	OST	PHMSA	SLSDC
Defined and communicated roles and responsibilities of stakeholders in information systems contingency planning (ISCP).	X	✔	X	✔	✔	X	✔	X	✔	✔	NT
ISCP program is defined and implemented through policies, procedures, and strategies.	✔	✔	X	✔	✔	X	X	✔	X	✔	X
Results of business impact analyses (BIA) are used to guide contingency planning.	X	X	X	X	X	X	X	X	X	X	NT
ISCPs are developed, maintained, and integrated with other continuity plans.	X	✔	X	X	X	X	X	X	✔	✔	NT
Performed tests/exercises of its ISCPs processes as required.	X	X	X	X	✔	X	X	X	X	✔	NT
Performed information system backup and storage, including use of alternate storage and processing sites.	X	X	X	X	✔	X	✔	X	X	✔	NT
Communicated information on planning and performance of recovery activities to internal stakeholders, executive management teams to make risk based decisions.	X	X	X	X	X	X	X	X	✔	✔	X

NT—Not tested. **X**—No ✔—Yes
* Contingency plan and testing requirements were derived from FY2017 IG FISMA Metrics questions.
Source: OIG analysis.

We found the following issues in OAs' implementation of DOT's contingency plans and testing requirements:

- FAA, FMCSA, MARAD, and OIG did not have roles and responsibilities of stakeholders involved in contingency planning defined and communicated;
- FMCSA, MARAD, NHTSA, and OST did not have defined and implemented contingency planning policies, procedures, and strategies as required by DOT's policy which states every OA is responsible for updating its policies and procedures to account for contingency planning policies;
- None of the 10 OAs tested ensured that the results of business impact analyses were documented and used to guide contingency planning efforts;
- FAA, FMCSA, FRA, FTA, MARAD, NHTSA, and OIG did not ensure that contingency planning is developed, maintained, and integrated with other continuity plans;
- FAA, FHWA, FMCSA, FRA, MARAD, NHTSA, OIG, and OST did not conduct annual contingency plan test and exercises as required;
- FAA, FHWA, FMCSA, FRA, MARAD, OIG, and OST did not identify alternative processing sites to perform information system backup and storage as appropriate; and
- Only 2 of the 11 tested OAs—OST and PHMSA—communicated information on planning and performance activities.

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

DOT relies on hundreds of information 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. DOT's cyber security program must protect these systems from malicious attacks or other compromises that may inhibit the Department's ability to carry out its functions and missions. While DOT has become adept at updating its policies and procedures, and consequently has achieved a defined level of maturity, we continue to find persistent deficiencies in processes such as system

reauthorization. These deficiencies place DOT's information systems at an increased risk of compromise and make them an easy target for malicious attackers.

Recommendations

To help the Department address the challenges in developing a mature and effective information security program, we recommend that the Chief Information Officer, take the following actions in addition to the prior open recommendations we identified in this report.

1. Require MARAD, NHTSA, OST, and SLSDC to develop and disseminate policies and procedures for their risk management programs that include the appropriate elements such as criteria for making risk based decisions.

2. Implement controls to verify that information on threat activity has been communicated to senior agency officials and require retention of supporting documentation.

3. For the COE and FAA, update procedures and practices for monitoring and authorizing common security controls to (a) require supporting documentation for controls continual assessments, (b) complete reauthorization assessments for the controls, (c) finalize guidance for customers' use of controls, and (d) establish communication protocols between authorizing officials and common control providers regarding control status and risks.

4. Verify that FAA's criteria regarding designation and definition of contractor systems conforms to DOT guidance, and that systems are correctly classified.

5. Implement controls to continuously monitor and work with components to ensure network administrators are informed and action is taken to disable system accounts when users no longer require access or have been inactive beyond established thresholds.

6. Complete PIV enablement and requirements for remaining information systems, except those that are subject to exclusions that are documented and approved.

7. Take action to fully implement mandatory use of PIV cards for VDI access.

8. Implement processes verifying that personnel performing certain security related roles receive specialized training needed to meet OCIO guidance.

Agency Comments and OIG Response

We provided DOT with our draft report on November 21, 2017, and received its response on December 20, 2017, which is included in its entirety as an appendix to this report. DOT concurs with recommendations 2, 4, 6, and 8 as written. DOT states that it plans to implement recommendation 4 by February 1, 2018, recommendation 2 and 8 by October 1, 2018, and recommendation 6, by December 1, 2020. DOT also concurs with recommendation 1 and proposes an alternative action to require DOT OAs to follow and implement Agency policy and processes, and develop and implement their own policies and processes by exception, as approved by the CIO. DOT plans to complete this action by October 1, 2018. DOT also concurs with recommendation 7 and proposes an alternative action to implement mandatory use of PIV cards or other Agency-approved multi-factor authentication, except in those instances subject to documented and approved exclusions. DOT plans to complete this action by December 1, 2019.

DOT concurs in part with recommendation 3, and acknowledges that the COE and FAA need to take action to implement policy within their programs. However, we disagree that DOT has already established complete policies and processes via the DOT Security Authorization and Continuous Monitoring Guide that specifically address this recommendation. As we indicate in this report, DOT's lack of comprehensive procedures and effective oversight of common controls could result in security incidents that go undetected.

DOT does not concur with recommendation 5, and states that this is a repeat finding for a prior recommendation that was closed by OIG in March 2017. However, DOT's actions did not appear effective because during our review we found various instances in which OAs did not have adequate mechanisms or controls to disable inactive accounts.

Actions Required

We consider recommendations 1, 2, 4, 6, 7 and 8 resolved but open pending completion of planned actions.

We request that DOT reconsider its position on recommendation 3, and identify the specific section or language and page numbers in the DOT Security Authorization and Continuous Monitoring Guide that provide evidence that the procedures and practices for monitoring and authorizing common security controls already exist and address the recommendation.

We request DOT reconsider its position on recommendation 5, and implement the recommendation effectively.

Exhibit A. Scope and Methodology

We conducted this performance audit between February and November 2017 in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. 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, 2016, and June 30, 2017. 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, 2017. We obtained a universe with 464 systems from CSAM repository the Department uses to track system inventories, weaknesses, and other security information. We divided this universe into 15 strata by OAs and risk categories. We computed sample sizes approximately proportionately but reduced the computed sample sizes to a minimum of two from each stratum unless there was only one and a maximum of nine in order to meet our statutory reporting deadline. We selected a stratified simple random sample of 44 out of 464 computer systems. During our audit we found that five systems in our universe were merged with existing systems, one was decommissioned, and one system that was not on our original list was added to the universe and sample, so that we reviewed a stratified sample of 45 out of 459 systems. Our sample design allowed us to estimate the percentage and number of non-compliant systems with NIST and DHS requirements in the

following areas: security authorization, contingency planning and testing, continuous monitoring, security control assessments and POA&Ms with a margin of error no greater than +/-14.2 percentage points at the 90 percent confidence level. Our margin of error is slightly larger than desired due to the small sample size, but still provided us with meaningful confidence limits. See table A for sampled systems and exhibit C for the system inventory.

We evaluated prior years' recommendations and supporting evidence to determine the progress 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; 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. OIG's Representative Subset of Sample Systems by OA

FAA

	System	Impact Level[a]	Contractor System[b]
1	Advanced Electronic Flight Strips	Low	Yes
2	Airport Surface Detection Equipment - Model X	Moderate	Yes
3	Airport Surveillance Radar – 11	Moderate	Yes
4	AJI Safety Applications System	Low	Yes
5	Aviation Safety Hotline Information System	Moderate	Yes
6	Aviation Safety Knowledge Management Environment Engineering Design and Production Approval	Moderate	Yes
7	Bandwidth Manager	Moderate	Yes
8	Business Management Solutions	Low	Yes
9	Certification and Compliance Management Information System .Net	Moderate	Yes
10	CountOps	Moderate	Yes
11	CRU-X	Moderate	Yes
12	Data Multiplexing Network	Moderate	Yes
13	Enterprise Management Tool Suite	Moderate	Yes
14	FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System	Low	Yes
15	FAA Transit Benefits Application/FAA Parking Application	Moderate	Yes
16	Flight Standards Information Management System	Moderate	Yes
17	Flight Standards Service Training Resource Information Manager	Moderate	Yes
18	Information System Security Services	Moderate	Yes
19	Intranet-Based Radio Coverage Analysis System	Low	Yes
20	National Airspace System Resource System	Low	Yes
21	Platform for Unified Reports for the Enterprise	Moderate	Yes
22	Print Request Information Tracking	Moderate	Yes
23	Wind Hazard Detection Equipment	Moderate	Yes

FHWA

	System	Impact Level[a]	Contractor System[b]
1	Fiscal Management Information System 5	Moderate	Yes
2	National Bridge Inventory System	Moderate	Yes
3	Video Conferencing System	Moderate	Yes

FMCSA

	System	Impact Level[a]	Contractor System[b]
1	FMCSA Cloud Environment	Moderate	Yes
2	National Complaint Hotline Database	Moderate	Yes

FRA

	System	Impact Level[a]	Contractor System[b]
1	Railroad Credit Assessment and Portfolio Management System	Moderate	No
2	Railroad Enforcement System	Moderate	No

FTA

	System	Impact Level[a]	Contractor System[b]
1	FTA Inter/Intranet	Moderate	Yes
2	Procurement Requisition Information System (PRISM)	Moderate	Yes

MARAD

	System	Impact Level[a]	Contractor System[b]
1	Maritime Service Compliance System	Moderate	Yes
2	RMS (Ready Reserve Force (RRF) Management System (RMS)	Moderate	Yes

NHTSA

	System	Impact Level[a]	Contractor System[b]
1	NHTSA501: CAFÉ	Moderate	Yes
2	NHTSA301: Teleprocessing & Timesharing Services NDR Program	Moderate	Yes

OIG

	System	Impact Level[a]	Contractor System[b]
1	Computer Crimes Unit Network	Moderate	No
2	US DOT OIG Infrastructure	Moderate	No

OST

	System	Impact Level[a]	Contractor System[b]
1	Consumer Complaints Application	Moderate	Yes
2	Cyber Security Assessment and Management	High	Yes
3	OST Airline Performance Economic Information System (APEIS)	Moderate	Yes
4	Volpe MSEPM (Microsoft Enterprise Project Management)	Moderate	Yes
5	Volpe Physical Access Control System	High	Yes

PHMSA

	System	Impact Level[a]	Contractor System[b]
1	Hazardous Materials Information System	Moderate	Yes
2	Safety Monitoring and Reporting Tool	Moderate	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. Organizations Visited or Contacted

Facilities

Office of the Secretary

Office of the Chief Information Officer

Federal Aviation Administration

Federal Highway Administration

Federal Motor Carrier Safety Administration

Federal Railroad Administration

Federal Transit Administration

Maritime Administration

National Highway Traffic Safety Administration

Office of Inspector General

Pipeline and Hazardous Materials Safety Administration

Saint Lawrence Seaway Development Corporation

Exhibit C. System Inventories for Fiscal Years 2016 and 2017, by OA

OA	FY 2016	FY 2017	Change
FAA	317	323	6
FHWA	17	16	(1)
FMCSA	16	19	3
FRA	11	12	1
FTA	8	8	-
MARAD	17	15	(2)
NHTSA	16	17	1
OIG	3	2	(1)
OST	43	44	1
PHMSA	7	7	-
SLSDC	1	1	-
Total Systems	**456**	**464**	**8**

Sources: CSAM as of January 30, 2017 and OIG analysis.

Exhibit D. Systems With Overdue Reauthorizations, by OA

OA	Asset	Total
FAA	Aeronautical Center Security Management System[a]	**33**
	Aerospace Accident - Injury Autopsy Data System (AA-IADS)	
	Airman Testing Standards (ATS)	
	Air Route Surveillance Radar Models 1 & 2[b]	
	Air Transportation Oversight System[a]	
	AML Logistics Center Local Area Network[a]	
	AST Local Area Network[b]	
	ATO Application Portal (AAP)	
	Aviation Camera System (AVCAMS)	
	Aviation Training Network[a]	
	Building Access, Software And Hardware For MMAC[b]	
	Common Controls Framework (CC)	
	Computer Based Instruction[a]	
	Conference Control System – Warrenton (CCS)	
	Dashboard (DASH)	
	Designee Information Network (DIN)	
	Designee Registration System (DRS)	
	Electronic File Service (EFS)	
	Enterprise Services Center Business Systems[a]	
	External Web Portal (EWP)	
	FAA Financial Disclosure System (FDOnline)	
	Facility Specific Safety Standard (FSSS)	
	Federal Data Registry (FDR)[a]	
	International Aviation Standards Data Exchange (IASDEX)	
	Mike Monroney Aeronautical Center Backbone Network (MMAC Net)	
	Mike Monroney Aeronautical Center Voice[a]	
	NAS Data Warehouse (NAS DW)	
	Office of Airport Local Area Network[b]	
	Quality Management Information Technology System (QMITS)	
	Recovery Communications System (RCOM)	
	Specials Waivers Inventory Management System (SWIMS)	

OA	Asset	Total
	System of Airport Reporting (SOAR)[a]	
	Whistleblower Protection Program (WBPP)	
FHWA	Central Federal Lands General Support System[a]	**5**
	Eastern Federal Lands General Support System[a]	
	Freedom Of Information Act System[b]	
	Procurement, Requisition Ordering (PRISM)[b]	
	Video Conferencing System[a]	
FMCSA	CDLIS-Gateway	**9**
	CoTs DOT LAN[b]	
	Customer Insurance and Registration Information Support (CIRIS)[a]	
	FMCSA LAN Segment at Volpe[b]	
	FMCSA Portal[a]	
	Licensing & Insurance[a]	
	Motor Carrier Management Information Systems (MCMIS)[a]	
	National Complaint Hotline Database (NCHDB)[b]	
	SAFETYNET[a]	
FTA	Safety Resource and Training System[a]	**1**
MARAD	BlackBoard[b]	**5**
	Cargo Preference (CAPOS)	
	Comprehensive Academic Management System[a]	
	MARAD Common Operating Environment (COE)	
	USMMA LAN[b]	
NHTSA	NHTSA Inventory System[a]	**4**
	NHTS320: Mission Information Protection Program (MIPP)P	
	PRISM[b]	
	WEB System[b]	
OST	Airline Reporting Data Information System[a]	**12**
	Case Tracking System[a]	
	Confidential Close Call Reporting System[b]	
	Correspondence Control Management System[a]	
	Facilities and Building Management System (FBMS)[b]	
	Grants Notification System (GNS)[a]	
	Library Systems[b]	
	RITA Web[b]	
	Security Operations Systems (SOS)[a]	
	Transtats[a]	

OA	Asset	Total
	WEB-enabled Emergency Operations Center (WebEOC)[b]	
	Web Printing System[a]	
PHMSA	PHMSA Portal System (PPS)	**1**
Total		**71**

[a] Reported in fiscal year 2016 FISMA with an expired Authorization-to-Operate, OA had updated ATO date and provided authorization documentation but it did not meet departmental re-authorization requirements.
[b] Reported in fiscal year 2016 FISMA with an expired Authorization-to-Operate, OA have not taken corrective action to re-authorize.
Source: CSAM as of June 11, 2017, and OIG analysis.

Exhibit E. Weaknesses in Configuration Management, by OA

FAA

System Name	Description of Weakness	Status	Planned Finish Date
AIT EDC	A secure baseline configuration has not been developed and maintained. The system does not have additional mechanisms defined specifically to detect and protect against unauthorized changes to software and information.	Delayed	9/30/2016
	Configuration change management processes have not been fully implemented to consistently test, validate, and document all system changes before implementing the changes on the operational system.	Delayed	9/30/2016
	Belarc is not currently deployed on all servers and devices. Therefore, the AIT EDC inventory documented in the FY16 AIT EDC System Characterization (SCD) is not complete. Additionally,	Delayed	9/30/2016
	The system owner does not review scan results on a regular basis.	Delayed	9/30/2017
	The Assessment Team examined the FY16 AIT EDC System Security Plan (SSP) and noted that it states "Windows and Unix/Linux servers are not securely configured in accordance with the Center for Internet Security (CIS) benchmarks.	Delayed	9/30/2016
	AIT EDC has not formally identified prohibited or restricted functions, ports, protocols, and/or services, resulting in AIT EDC not completely configuring the system to provide only essential capabilities and prohibiting or restricting the use of specified functions, ports, protocols, and/or services.	Delayed	9/30/2016

System Name	Description of Weakness	Status	Planned Finish Date
AIT Networks	Facility staff do not maintain a site specific inventory. There are no procedures to update the inventory on regular basis no controls are in place to reconcile physical inventory against assets captured through automated mechanisms.	Delayed	9/30/2016
	Privileged access (write) authorization is not currently provided to the SOC for vulnerability scanning. In addition, the assessors found a large number of assets listed on the system inventory are not scanned on a monthly basis.	Delayed	9/30/2016
	Cisco ACS, Active Directory DNS, Forescout NAC, switches & routers, and Wireless Network Infrastructure undergo ad-hoc audits to identify unnecessary and/or non-secure functions, ports, protocols, and services.	Planned/Pending	9/30/2017
AVS Infrastructure	The AVS infrastructure does not employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of AVS infrastructure servers and other hardware that supports applications.	Delayed	9/30/2016
	Although the Change Request Tool and MKS fully automates the change control process for hosted applications, the SCCM tool automated functionality is not fully implemented for AVS infrastructure hardware components.	Delayed	9/30/2016
	The System Owner has not produced a checklist to assist with verifying potential security impacts resulting from configuration changes. The team found that changes are not verified either manually or through automated mechanisms.	Delayed	12/30/2016
	AVS does not have a process for assigning each vulnerability to responsible parties and tracking and reviewing those findings to completion.	Delayed	9/30/2016
	The majority of applications hosted in the EDC (ARB) contain flaws that have been identified during scanning associated with multiple assessments. Depending on the application owners to correct these flaws has resulted in the EDC (ARB) operating at a significant level of risk. A patch management process is not fully in place for the servers hosted in the EDC (ARB).	Delayed	9/30/2016

System Name	Description of Weakness	Status	Planned Finish Date
FAA AFN - AIT CRU-X	A software assurance assessment has not been performed on the CRU-X application.	Delayed	9/30/2017
	The vulnerability scan report dated November 22, 2016 identified nine (9) High findings and (5) medium vulnerabilities. The high findings identified two (2) unique vulnerabilities related to not having SSL implemented. (Insecure Transport, Unencrypted Login Form); T	Planned/Pending	9/30/2017
FAA AFN - ARC FAA Transit Benefits Application/FAA Parking Application	There is no evidence that a Webinspect vulnerability scan was completed (finding entered into CSAM 8/13/2015).	Delayed	3/31/2014
	There is no evidence that the system provides only essential capabilities and specifically prohibits or restricts the use of functions, ports and/or protocols.	Delayed	7/1/2014
	The system owner does not develop, document and maintain under configuration control, a current baseline configuration of the system.	Delayed	8/1/2014
	The system owner does not (1) manage all aspects of configuration change control procedures, (2) perform security impact analysis as part of configuration changes, (3) document approved configuration changes, and (1) review records and audit activities regarding configuration changes.	Delayed	8/1/2014
	There is no configuration management document related to backup control implementation. Control implementation points to a baseline not pertaining to this system.	Delayed	8/1/2014
FAA AFN - FFO 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.	Delayed	6/25/2017
	System owners must centrally manage the flaw remediation process and install software updates. The system owner has not remediated critical vulnerabilities.	Delayed	8/3/2016

System Name	Description of Weakness	Status	Planned Finish Date
FAA AFN - FFO Information System Security Services	Scans provided during the assessment do not demonstrate the use of credentialed access. The last credential scan on the production/test web environment was done over a year ago, non-credential are done monthly. The assessors also found four vulnerabilities that are 90+ days overdue for remediation.	Delayed	6/13/2016
FAA ARP CCMISNet (Certification and Compliance Management Information System .Net)	Vulnerability scans for this assessment were not conducted.	Delayed	6/30/2017
	There were no scans conducted during this assessment cycle and no way to prove that flaws were remediated.	Delayed	6/30/2017
FAA ATO NAS AEFS (Advanced Electronic Flight Strips)	Testing revealed the system is not configured to provide only the required ports, protocols, and/or services. The Latest Nessus scan revealed 10 high and 32 medium vulnerabilities.	Not found in CSAM	3/24/2017
	The SSP does not address the requirements of the control. The SSP only states that this control is not implemented. Testing revealed that AEFS assets have not been hardened according to checklists (for security patches, account policy settings, and security options settings) provided on the ATO ISS Program website.	Not found in CSAM	5/1/2017
	The SSP indicates that flaw remediation is not implemented. Testing showed the Windows devices have not been updated and are missing many Windows patches.	Not found in CSAM	5/1/2017
FAA ATO NAS ASDE-X (Airport Surface Detection Equipment - Model X)	The System Characterization Document (SCD), dated December 2015, has been submitted in support of the FY16 ISCM assessment; however, it does not represent the current configuration.	Not found in CSAM	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
FAA ATO NAS DMN (Data Multiplexing Network)	The DMN system is not configured to provide only the required ports, protocols, and services and is comprised of unsupported assets, which connect to the OPIP network periodically. The scan results indicated 8 critical, 8 high and 14 medium vulnerabilities.	Not found in CSAM	11/30/2016
	The DMN SSP does not document how flaw remediation is performed in relation to the Configuration Management Process.	Not found in CSAM	11/30/2016
FAA ATO NAS NASR (National Airspace System Resource System)	The NASR System Characterization Document does not contain a complete inventory of components. it also does not identify the assets found during a scan review from the previous assessment.	Not found in CSAM	3/31/2017
	ATO does not fully implement and maintain mandatory configuration settings in accordance with the applicable Secure Configuration Baseline Standards. Nessus Credentialed scans performed against Solaris discovered many non-compliant items.	Not found in CSAM	6/30/2017
	NASR assets have open, potentially unneeded ports enabled. The Nessus scan tool discovered active ports with vulnerabilities. The most recent Nessus scan was performed on April 5, 2016 and discovered 1 critical, 23 high and 46 medium vulnerabilities.	Not found in CSAM	6/30/2017
FAA ATO NAS WHDE (Wind Hazard Detection Equipment)	The SSP does not currently specifically address the ports, protocols, services and physical devices required to be active on each WHDE asset to support system operation.	Not found in CSAM	1/2/2016
FAA ATO non-NAS AJI Safety Applications System	Based on the results from WebInspect testing, a number of system flaws have been identified requiring mitigation. Identified deficiencies include but are not limited to the following: Cross-Frame Scripting, Cookie Security, System Information Leaks, and Unprotected Files. Cross Site Scripting issue across many files.	Not found in CSAM	12/30/2016

System Name	Description of Weakness	Status	Planned Finish Date
FAA ATO non-NAS CountOps	The types of changes that are under configuration control are not defined in the System Security Plan (SSP) under CM-03.a. The change control entity authorized to review and approve configuration-controlled changes to the system is not documented in the SSP under CM-03.b.	Not found in CSAM	9/30/2017
	According to the SSP, CountOps is not configured to meet all DOT security web application standards. Based on results from WebInspect scan testing, a number of security issues have been identified requiring mitigation.	Not found in CSAM	9/30/2017
	The SSP states CountOps alerts CSMC during any security relevant changes to the system, but no procedures are currently documented for reporting security incidents.	Not found in CSAM	9/30/2017
	The CountOps System Characterization Document does not clearly describe the assets within the authorization boundary.	Not found in CSAM	Not Specified
FAA ATO non-NAS Enterprise Management Tool Suite	The SSP states that the system owners implement security relevant software updates provided by AIT but does not list a time frame of implementing these updates. The SSP does not document processes for flaw remediation.	Not found in CSAM	2/28/2017
	System Owner is updating documentation for this Configuration Management procedure in accordance with the ATO ISS Procedures Guidance and to incorporate EMT Passport. The SSP states that the OS level is handled by the MMAC but fails to document the control adequately for the application level.	Not found in CSAM	9/30/2017
FAA ATO non-NAS FEATS (FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System)	The assessors found many system inventory discrepancies in the System Characterization Document, including system assets used for development, pre-preproduction and production are not part of the FEATS authorized boundary.	Not found in CSAM	9/30/2016
	The FEATS authorization boundary contains Windows Server 2003, which is no longer supported.	Not found in CSAM	3/31/2017

System Name	Description of Weakness	Status	Planned Finish Date
	Based on results for Web Inspect scan testing, a number of system flaws have been identified requiring mitigation. Identified deficiencies include but are not limited to the following: Cross-Frame Scripting, Credential Management: Insecure Transmission and Session Fixation.	Not found in CSAM	Not Specified
FAA AVS ASHIS (Aviation Safety Hotline Information System)	The ASHIS environment is not regularly scanned, reviewed or remediated within required FAA timeframes. A lack of regular vulnerability scanning, analysis and remediation compromises efforts to identify, disable and uninstall unused or unnecessary ports, protocols, services and applications.	Delayed	9/30/2016
	AVS workstations scans are rarely performed, as most POCs responsible for components depend on the on-demand scanning capability. AVS does not have a process for assigning each vulnerability to responsible parties and tracking and reviewing those findings to completion.	Delayed	9/30/2016
	The ASHIS environment is not regularly scanned, reviewed or remediated within required FAA timeframes. Servers on a "no patch" list are not automatically patched and software updates are not automatically installed.	Delayed	9/30/2016
	The documents for the AVS infrastructure components and platforms have not been maintained. AVS manages the baseline security configuration using virtual machine templates originally configured based on the AVS BSCS documents. However, the template configuration is not documented. A POAM item has been created to track remediation of this finding.	In Progress	7/31/2017
FAA AVS Aviation Safety Knowledge Management	ASKME Configuration Management Plan (CMP) does not reflect the current baseline configuration of the system.	Delayed	6/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
Environment Engineering Design and Production Approval	Some servers are added to a "no patch" list because of possible compatibility issues with legacy applications. While these patches are generally addressed, there is some inconsistency in follow through; therefore, some servers have vulnerabilities that were identified but not remediated.	Delayed	6/30/2017
	The FAA SOC scans Web applications using the HP WebInspect tool. Typically, a WebInspect scan is performed in conjunction with a security assessment; however, System Owners may request scans as part of their change management processes.	Delayed	9/30/2017
FAA AVS FSIMS (Flight Standards Information Management System)	FSIMS does not implement a continuous monitoring strategy which includes conducting ongoing assessments of accounts for deletion, modification or evidence of inappropriate activity at least quarterly. FSIMS does not employ automated mechanisms to support the management of privileged accounts or auditing of accounts in the FSIMS data administrator group. These accounts are managed manually and are not disabled after a period of inactivity. FSIMS does not limit concurrent sessions.	Delayed	9/30/2016
	WebInspect scans are not conducted for IBM Lotus Domino or SharePoint Services-based applications.	Delayed	5/31/2017
FAA Platform for Unified Reports for the Enterprise (PURE)	The system does not generate automatic alerts when new accounts are created, modified, or removed on servers, Tableau, Qlikview, Domo, Business Objects, SOA, and Pure Portal.	Delayed	6/30/2016
	Application, server and database functions, ports, protocols and services required by the system have not been identified and documented. Functions, ports, protocols and services are not reviewed on a quarterly basis to identify and disable unnecessary or nonsecure settings.	Delayed	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
	Scans for PURE servers, databases and application were performed and provided. However, not all devices within the PURE boundary were scanned. There was no evidence that the following production and non-production URL's were scanned in the last year.	Delayed	9/30/2017
	Baseline configurations are reviewed and updated when significant changes occur to the COTS and are not reviewed in an annual basis per the DOT Cybersecurity Compendium.	Planned/Pending	8/31/2017
	The Assessment team is unable to determine if remediation is taking place for the absent URL scan results.	Planned/Pending	9/30/2017
FAA Telecommunications Infrastructure (FTI)	Security-relevant software updates are not implemented in all cases based on asset location as described.	Delayed	8/31/2017
	Not all CIS mandatory configuration settings for all OT products employed on the program are maintained. Information systems are configured in accordance with current configuration standards. Not all of the exceptions from the CIS checklists are documented for FTI.	Delayed	9/30/2017
MMAC NET	The information system does not perform monthly scans on all information system components. Therefore, it is also undetermined if all vulnerabilities are remediated within DOT Compendium defined timeframes.	Delayed	12/30/2016
	The organization does not consistently implement DOT OCIO approved security configuration checklists. These checklists include whitelisted and blacklisted ports, protocols, services and functions. Moreover, the organization does not identify, document and approve any deviation from the established DOT OCIO approved security configuration checklists. Deviations exist that are not documented or controlled.	Planned/Pending	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
	Information system components are not configured in accordance with approved DOT OCIO security configuration baseline standards, and as such this control is not implemented.	Planned/Pending	9/30/2017
	The organization does not employ integrity verification tools to detect unauthorized changes to software, firmware, and information. Moreover, the organization does not perform an integrity check of software, firmware, and information annually. Additionally, the organization does not use automated mechanisms with a maximum five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system.	Planned/Pending	9/30/2017
MMAC TIC	The information system does not perform monthly scans on all information system components. Therefore, it is also undetermined if all vulnerabilities are remediated within DOT Compendium defined timeframes. The information system does not perform monthly privileged scans on all information system components. Privileged credentials have been provided by the system owner to the FAA SOC.	Delayed	12/30/2016
	The organization does not employ an automated mechanism/tool to manage changes to and maintenance activity on the information system.	Planned/Pending	9/30/2017
	Information system components are not configured in accordance with approved DOT OCIO security configuration baseline standards, and as such this control is not implemented.	Planned/Pending	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
	The organization does not employ integrity verification tools to detect unauthorized changes to software, firmware, and information. Moreover, the organization does not; perform an integrity check of software, firmware, and information semi-annually; automatically perform or implement a security safeguard when integrity violations are discovered; or automatically notify personnel upon discovering discrepancies during integrity verification. Additionally, the organization does not use automated mechanisms with a maximum five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system.	Planned/Pending	9/30/2017
	Information system components are not configured in accordance with approved DOT OCIO security configuration baseline standards, and as such this control is not implemented.	Planned/Pending	9/30/2017
WJHTC TIC	Currently, only a portion of WJHTC TIC systems are being scanned by the FAA SOC. The scans are not conducted on monthly basis.	Not found in CSAM	Not Specified

OST

System Name	Description of Weakness	Status	Planned Finish Date
COE	Remote devices are not scanned for malware prior to be granted connection to the system or network.	Delayed	11/30/2017
	The COE does not mandate each OA to mitigate vulnerabilities in its system or remove the systems from the network.	Delayed	3/31/2014
	The COE does not ensure that system owners perform regular vulnerability assessments of all internal systems to identify known vulnerabilities and common misconfigurations.	Delayed	9/30/2015

System Name	Description of Weakness	Status	Planned Finish Date
	The COE does not maintain a complete inventory of authorized network devices.	Delayed	3/31/2014
Volpe Center GSS/LAN	Temporary accounts are not automatically removed/disabled after a predefined period. Privileged accounts and associated privileges are not regularly reviewed to ensure accounts are commensurate with job function, need-to-know, and contractor/employee status.	Not Started	TBD
	A review of the PIV access exemption report indicates multiple users have been granted "permanent" exemptions without documented justifications. The report identified users with an exemption status beyond the authorized expiration date.	Not Started	TBD

FMCSA

System Name	Description of Weakness	Status	Planned Finish Date
FMCSA Motor Carrier Management Information Systems	The System Security Plan (SSP) does not describe the process for reissuing shared/group account credentials when individuals are removed from the group. In addition, evidence was not provided to show that the system automatically disables inactive accounts after 90 days of inactivity.	FMCSA reported the MCMIS system has been merged into FMCSA CE (Cloud Environment) as a subsystem. Therefore, the POAMs are managed under FMCSA CE. Due to quantity from the 2016 assessment, the FMCSA CE POAMs are managed outside of CSAM. Correction Plan: After completion of the 2017	
	The system does not have a fully developed and documented secure baseline configuration.		
	The software inventory documented in the SSP is incomplete. Therefore, assessors could not validate mechanisms employed to allow secure execution of authorized software programs. Evidence was not provided to demonstrate that changes to the system to disable unnecessary services were performed.		
	Due to an incomplete hardware, software, and firmware list - assessment of this control could not be validated to ensure that components within the authorization boundary of the information system are not duplicated in other system inventories.		

System Name	Description of Weakness	Status	Planned Finish Date
	Evidence demonstrating that software/firmware updates are installed within the 30 days of the release of the updates does not exist.	annual assessment for the FCMSA CE, all the appropriate POAMs will be entered or closed in CSAM by the 3PAO/ISSM as required. Assessment completion schedule for Nov 20, 2017.	
FMCSA National Complaint Hotline Database (NCHDB)	The system does not have a fully developed secure baseline configuration.	FMCSA reported after completion of the 2017 annual assessment for the NCHDB, all appropriate POAMs will be entered/managed in CSAM by the 3PAO/ISSM as required.	
	The NCHDB service provider does not consistently document approved configuration-controlled changes to the system.		
	Firewalls have not been fully configured in accordance with Center for Internet Security (CIS) benchmarks.		
	During the last security control assessment, assessors noted the NCHDB Contact Center: • continues to utilize versions of Adobe Acrobat that are currently not supported, • does not test software updates for effectiveness and potential side effects on systems before installation, • does not incorporate flaw remediation into the organizational configuration management process as configuration/change management processes have not been established.		

FRA

System Name	Description of Weakness	Status	Planned Finish Date
FRA Railroad Credit Assessment and Portfolio Management System	There is no process to validate and refresh system images used to deploy systems and virtual machines. Integrity checking tools are not defined on server that contains master images to ensure unauthorized changes have not been made. According to the SSP, this is a hybrid control. The baseline configuration for the OS and database are out of scope for the RCAPM system administrators. They are maintained by the FRA system engineers responsible for maintaining that aspect of applications that leverage services from the common control provider.	Not found in CSAM	Not Specified
	A configuration baseline has not been established for supporting Windows and database servers through FRA HOSTS. Baseline deviations are documented but not approved. FRA reported this is a hybrid control and the weakness is derived from the common control provider.	Not found in CSAM	Not Specified
FRA Railroad Enforcement System (RES)	There is no formal review process for user accounts and auditable events. These reviews are performed on an ad hoc basis. The application does not have the capability to audit the execution of privileged functions within the application.	Planned/Pending	10/15/2017
	The system owner has not produced any versions of the baseline configuration. The RES does not have a documented configuration management plan that should address roles, responsibilities and configuration management processes/procedures.	Planned/Pending	10/15/2017

FTA

System Name	Description of Weakness	Status	Planned Finish Date
FTA Inter/Intranet	No evidence of deviations, to designated benchmarks, being documented or approved was provided. It is unclear how unauthorized security-relevant configuration changes are detected and designated personnel are being alerted, within the required timeframe and until it is investigated.	Not found in CSAM	Not Specified
	WebInspect scans were not provided for all components of WebApps during the time of the assessment.	Not found in CSAM	Not Specified

MARAD

System Name	Description of Weakness	Status	Planned Finish Date
MARAD RMS (Ready Reserve Force (RRF) Management System (RMS)	A configuration baseline is not developed, documented, or maintained for RMS. RMS does not define the number of previous baseline configurations which must be kept in order to support rollback.	Not Started	Not Specified
	Proposed configuration-controlled changes within RMS are not reviewed, approved /disapproved, and documented. RMS does not test, validate, and document changes to the information system before implementing the changes on the operational system.	Not Started	Not Specified
	The SSP does not define specifically which security configuration checklists are to be used for RMS components.	Not Started	Not Specified
	The SSP does not define prohibited or restricted software programs, functions, ports, protocols, and/or services to ensure system integrity.	Not Started	Not Specified

System Name	Description of Weakness	Status	Planned Finish Date
	MARAD could not demonstrate that the RMS component inventory is updated during installations/removals. The SSP does not define the frequency at which automated mechanisms to detect hardware, software, and firmware components are conducted. Not all servers within RMS boundary are being scanned for unauthorized hardware, software, and firmware. The SSP does not define personnel or roles to be notified when unauthorized components are detected.	Not Started	Not Specified
	Not all RMS servers are being scanned on a monthly basis. There is no evidence that vulnerability scan reports and risk assessment results are periodically reviewed. Remediation of moderate vulnerabilities is not mitigated within established timeframes. Plan of Action and Milestones (POA&Ms) are not entered into CSAM for vulnerabilities discovered during scanning and are not mitigated within defined timeframes. Privileged access to RMS components has not been defined/authorized for select vulnerability scanning activities.	Not Started	Not Specified
	Automated mechanisms are not employed in regards to flaw remediation within RMS.	Not Started	Not Specified
USMMA LAN	Multifactor authentication for privileged accounts is not in place. Multifactor authentication for local and/or network access to privileged accounts is not documented and implemented.	Delayed	7/31/2016
	Situations that require remote access to privileged functions are not defined. Usage restrictions and implementation guidance for organization-controlled wireless devices is not implemented.	Delayed	1/2/2017
	Inactive user accounts are not automatically disabled after a defined timeframe.	Delayed	1/2/2017

OIG

System Name	Description of Weakness	Status	Planned Finish Date
OIG US DOT/OIG Infrastructure	Vulnerability scanning is not being conducted in accordance with organizational policy. OIG reported they are on track for remediating this weakness by 11/26/2017.	In Progress	8/23/2017

PHMSA

System Name	Description of Weakness	Status	Planned Finish Date
PHMSA Safety Monitoring and Reporting Tool	Not all required access controls are implemented per organizational policy. Currently, SMART does not individually log or maintain within the current user account auditing model to include enabled and disabled account events. Also SMART does not notify responsible personnel of account actions including modification, enabling and disabling. In a recent meeting with the OIG, PHMSA stated they are on track for resolving this weakness by the planned finish date.	Not Started	12/26/2017

Source: OIG analysis.

Exhibit F. Weaknesses in User Identity Authentication and Access Management, by OA

FAA

System Name	Description of Weakness	Status	Planned Finish Date
AIT EDC	A centralized management mechanism is not in place for Unix and Linux privileged accounts.	Delayed	9/30/2016
	Not all AIF-330 assets display a warning banner as part of every system login, as required by DOT policy.	Delayed	9/30/2016
	Multifactor authentication is not fully deployed for local access for privileged accounts on all servers.	Delayed	9/30/2016
AIT Networks	AIT Networks utilizes a single local Administrator account for switches and routers for emergency purposes when remote access is unavailable. The credentials to this account remain static and are not changed.	Delayed	9/30/2016
AVS Infrastructure	The Assessment Team determined (1) the system does not have a defined process for creating, enabling, modifying, disabling, removing, reviewing, and monitoring of privileged accounts for the system, (2) the privileged system-level accounts are not reviewed on a regular basis and the use of privileged accounts is not being monitored, and (3) the system does not have a centralized management mechanisms is not in place for Unix and Linux privileged accounts.	Delayed	9/30/2016
	Multifactor authentication is not employed for network access to privileged accounts.	Delayed	9/30/2016
FAA AFN - AIT CRU-X	The application does not have built-in logging. CRU-X account creation, modification, enabling and disabling is not audited and there are no automatic notifications of these events. CRU-X does not audit the execution of privileged functions. This can have adverse impacts on the system if unauthorized users are granted access.	Delayed	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
FAA AFN - ARC FAA Transit Benefits Application/FAA Parking Application	System does not incorporate automated mechanisms to disable inactive accounts, audit accounts, or notify appropriate individuals of account management activities. In addition, there are no standard operating procedures on creating user accounts.	Delayed	7/1/2014
	IS3 does not establish conditions for role membership. The assessors also found that accounts with administrative privileges (including local administrator rights) are not expressly prohibited from web browsing and other Internet connections outside of the local protected boundary unless such risk is accepted in writing by the DOT Component CIO.	Delayed	6/13/2016
FAA AFN - FFO Business Management Solutions	There is no evidence that accounts of personnel no longer requiring access to the BMX application are deactivated and BMX users are reviewed in accordance with DOT policy.	Delayed	6/25/2017
FAA ARP CCMISNet (Certification and Compliance Management Information System .Net)	The information systems do not remove or disable the temporary or emergency accounts within a set time frame. The information systems do not automatically audit the following account actions creation; modification; enabling; disabling; removal. The organization has not employed an automated account management process for the information system. Both information systems can disable inactive accounts but they cannot create, modify or remove accounts via an automated process.	Delayed	6/30/2017
FAA ATO NAS AEFS (Advanced Electronic Flight Strips)	Per the SSP, account managers review user accounts semiannually and disable unused accounts in accordance with AEFS Security Procedures. However, the SSP does not document the review of privileged accounts. Procedures for reissuing shared/group account credentials when individuals are removed from the group are not defined in AC-01.ab.2. The SSP states that AEFS is waiting on mapped drive issue resolution prior to implementation.	Not found in CSAM	3/24/2017

System Name	Description of Weakness	Status	Planned Finish Date
FAA ATO NAS ASDE-X (Airport Surface Detection Equipment - Model X)	Procedures for account creation have not been formally defined and documented. It is uncertain if System Account Managers follow procedures in accordance with ATO ISS requirements. The SSP dated March 2015 does not document procedures that describe the account manager responsibilities when the following conditions occur: 1. When users are terminated or transferred 2. When individual information system usage or need-to-know changes. Procedures have not been defined in AC-02.e. The SSP is only addressing procedures performed by ASH. There are no specific procedures in place addressing the reissue of group credentials when individuals are removed from the group.	Not found in CSAM	Not Specified
FAA ATO NAS DMN (Data Multiplexing Network)	DMN System Account Managers do not review system level user accounts annually and privileged user accounts semi-annually, and initiate required actions based upon the review. System account procedure does not include process and responsibilities for reviewing system accounts. Procedures for reissuing shared/group account credentials when individuals are removed from the group are not documented in the DMN SSP.	Not found in CSAM	11/30/2016
FAA ATO NAS NASR (National Airspace System Resource System)	Based on the examination of the SSP dated March 2016 and the AIM-I AC SOP, procedures for reissuing shared/group account credentials when individuals are removed from the group are not addressed.	Not found in CSAM	12/31/2016
FAA ATO non-NAS AJI Safety Applications System	The SSP does not address key components of access control. It does not address the requirement to automatically disable inactive user accounts after 90 days of inactivity. The SSP does not identify types of accounts used. The SSP does not identify the personnel responsible for account management and or describe how accounts are managed. The SSP does not indicate how often account reviews are conducted. The SSP does not provide a reference to documented procedures.	Not found in CSAM	11/15/2016

System Name	Description of Weakness	Status	Planned Finish Date
FAA ATO non-NAS CountOps	The CountOps SSP does not address how often System Account Managers review user accounts and the actions that are initiated based upon the review. The SSP only states that CountOps system level Access Control is automated and described in the COT SOP, "User Account Management" section.	Not found in CSAM	9/30/2017
FAA ATO non-NAS Enterprise Management Tool Suite	The SSP states that operating system accounts are handled by the MMAC but fails to document the control adequately for application specific accounts.	Not found in CSAM	FY 2017
FAA ATO non-NAS FEATS (FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System)	The SSP fails to document (1) access privileges associate with each account type, (2) whether emergency or temporary user accounts are used, and (3) if disabling is done within 24 hours after determining the account is no longer needed.	Not found in CSAM	9/30/2016
FAA Platform for Unified Reports for the Enterprise (PURE)	The system does not generate automatic alerts when new accounts are created, modified, or removed on servers, Tableau, Qlikview, Domo, Business Objects, SOA, and Pure Portal.	Delayed	6/30/2016
MMAC NET	The assessment team determined that multifactor authentication has not been implemented for local access. The assessment team determined that replay resistant authentication has not been implemented for network access.	In Progress	9/30/2017
	The information system does not automatically disable inactive accounts after 90 days for all users across all information system components. The information system only performs this on the Windows servers. The organization did not provide evidence to demonstrate that the information system automatically audits events across the following platforms: Solarwinds, Access Control server (ACS), Windows servers. Additionally, the organization does notify defined personnel and roles of account creation, modification, enabling, disabling, and removal actions across all information system components.	Planned/Pending	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
	Evidence was not provided that the DOT required warning banner language is implemented on the ACS server.	Planned/Pending	9/30/2017
MMAC TIC	MMAC TIC does not implement multifactor authentication for network access. The MMAC TIC does not implement replay resistant authentication for network access. The organization implements PIV authentication on the Juniper VPN client access. Other than that, the organization does not implement multifactor authentication on the information system. This includes network and local access, for privileged and un-privileged accounts.	Delayed	9/30/2016
	Information system components disable inactive accounts after 90 days. However, this is not performed automatically across all information system components.	Not found in CSAM	9/30/2017

OST

System Name	Description of Weakness	Status	Planned Finish Date
COE	Multifactor authentication is not implemented on remote access to the Virtual Desktop Infrastructure. Not all COE information systems are PIV enabled.	Delayed	11/30/2017
Volpe Center GSS/LAN	Temporary accounts are not automatically removed/disabled after a predefined period. Privileged accounts and associated privileges are not regularly reviewed to ensure accounts are commensurate with job function, need-to-know, and contractor/employee status.	Not Started	TBD
	A review of the PIV access exemption report indicates multiple users have been granted "permanent" exemptions without documented justifications. The report identified users with an exemption status beyond the authorized expiration date.	Not Started	TBD

FMCSA

System Name	Description of Weakness	Status	Planned Finish Date
FMCSA Motor Carrier Management Information Systems	The System Security Plan (SSP) does not describe the process for reissuing shared/group account credentials when individuals are removed from the group. In addition, evidence was not provided to show that the system automatically disables inactive accounts after 90 days of inactivity. FMCSA reported the MCMIS system has been merged into FMCSA CE (Cloud Environment) as a subsystem. Therefore, the POAMs are managed under FMCSA CE. Due to quantity from the 2016 assessment, the FMCSA CE POAMs are managed outside of CSAM.	After completion of the 2017 annual assessment for the FCMSA CE, all the appropriate POAMs will be entered or closed in CSAM by the 3PAO/ISSM as required. Assessment completion schedule for Nov 20, 2017.	
FMCSA National Complaint Hotline Database (NCHDB)	FMCSA has not demonstrated compliance with DOT account management policies and procedures. Specifically, • The account creation, disable, and removable process is not fully documented to ensure that roles and responsibilities are clearly delineated. • There is no process to ensure the accounts of users who are terminated, transferred, or no longer require access are properly disabled within the defined timeframe. • Formal records of account authorization and access provisioning is not currently maintained for audit purposes. • The SSP does not document shared/group account credentials used within the environment. • FMCSA could not demonstrate the system automatically disables inactive accounts and initiates a session lock after a defined period of inactivity.	FMCSA reported after completion of the 2017 annual assessment for the NCHDB, all appropriate POAMs will be entered/managed in CSAM by the 3PAO/ISSM as required.	
	FMCSA does not define the frequency to re-sign access agreements to maintain access to organizational information systems when access agreements have been updated. Evidence to support compliance with the 24-hour requirement to terminate system access when users are terminated and authenticators/credentials are revoked was not provided.		

FRA

System Name	Description of Weakness	Status	Planned Finish Date
FRA Railroad Enforcement System (RES)	There is no formal review process for user accounts and auditable events. These reviews are performed on an ad hoc basis. The application does not have the capability to audit the execution of privileged functions within the application.	Planned/Pending	10/15/2017

FTA

System Name	Description of Weakness	Status	Planned Finish Date
FTA Inter/Intranet	Automated notifications for account creation, modification, enabling, and removing are not in place.	Delayed	5/29/2015

MARAD

System Name	Description of Weakness	Status	Planned Finish Date
MARAD RMS (Ready Reserve Force (RRF) Management System (RMS)	The SSP does not specify account managers responsible for user accounts, authorized users and associated privileges and roles. Procedures have not been established for account management. MARAD has not demonstrated that account managers are being notified when accounts are no longer required, users are terminated or transferred, and/or an individual user's need to know changes. User accounts are not disabled after 90 days of inactivity and accounts are not regularly audited.	Not Started	TBD
USMMA LAN	Multifactor authentication for privileged accounts is not in place. Multifactor authentication for local and/or network access to privileged accounts is not documented and implemented.	Delayed	7/31/2016
	Situations that require remote access to privileged functions are not defined. Usage restrictions and implementation guidance for organization-controlled wireless devices is not implemented.	Delayed	1/2/2017

System Name	Description of Weakness	Status	Planned Finish Date
	Inactive user accounts are not automatically disabled after a defined timeframe.	Delayed	1/2/2017

OIG

System Name	Description of Weakness	Status	Planned Finish Date
OIG US DOT/OIG Infrastructure	During the last security assessment, assessors noted that OIG does not: - Create privileged accounts that are restricted from using e-mail and the internet. - Create, enable, modify, disable and remove system accounts in accordance with organizational policy. - Automatically notify account managers when accounts are created, modified, enabled, disabled or removed. - Define the time period after which temporary and guest accounts are automatically disabled or removed. - Consistently disable network accounts after a defined period of inactivity. In addition, procedures are not in place for reissuing shared/group account credentials when individuals are removed from the group.	In Progress. On 9/12/2017 OIG created a new POAM to address findings from 2016 that were not completed within DOT required timeframes. OIG reported they are on track for remediating these weaknesses by 2/1/2018.	

PHMSA

System Name	Description of Weakness	Status	Planned Finish Date
PHMSA Safety Monitoring and Reporting Tool	Not all required access controls are implemented per organizational policy. Currently, SMART does not individually log or maintain within the current user account auditing model to include enabled and disabled account events. Also SMART does not notify responsible personnel of account actions including modification, enabling and disabling. In a recent meeting with the OIG, PHMSA stated they are on track for resolving this weakness by the planned finish date.	Not Started	12/26/2017

Source: OIG analysis.

Exhibit F. Weaknesses in User Identity Authentication and Access Management, by OA

Exhibit G. Weaknesses in Incident Response, by OA

FAA

System Name	Weakness Description	Status	Planned Finish Date
AIT EDC	AIT EDC's incident handling capability does not consistently notify AIF-330 personnel of security incidents.	Delayed	9/30/2016
	The Assessment Team has determined that an incident response process has not been developed, documented, and implemented for AIT EDC.	Delayed	9/30/2016
AIT Networks	AIT Networks does not utilize automated mechanism to support the incident reporting process.	Delayed	9/30/2016
AVS Infrastructure	The Assessment Team determined that the organization does not have a documented incident response plan.	Delayed	9/30/2016
FAA ARP CCMISNet	An incident response plan has not been implemented for the CCMISNet (Certification and Compliance Management Information System .Net).	Delayed	6/30/2017
FAA ATO NAS ASDE-X	The ASDE-X (Airport Surface Detection Equipment - Model X) Incident Response Procedures have not been developed and documented. The referenced documentation in the SSP has not been submitted for review. It is uncertain if these documents include process and responsibilities for reporting security incidents to the NCO or CSMC.	Not found in CSAM	Not Specified
FAA ATO non-NAS CountOps	The system alerts CSMC during any security relevant changes to the system, but no procedures are currently documented for *reporting* security incidents.	Not found in CSAM	9/30/2017

System Name	Weakness Description	Status	Planned Finish Date
FAA ATO non-NAS Enterprise Management Tool Suite	Based on the examination of the SSP dated January 2016, system level incident response procedures that pertain to ATO ISS Procedures Guidance are not referenced by title or number.	Not found in CSAM	2/28/2017
FAA ATO non-NAS FEATS	The ATO non-NAS FEATS (FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System) SSP does not adequately address Incident response procedures. SSP merely states "The ATO Enterprise Incident Response Team has established a Centralized Event Management (CEM) working group to develop an incident response support resource for systems."	Not found in CSAM	Not Specified
WJHTC TIC	WJHTC TIC does not utilize automated mechanism to support the incident reporting process.	In Progress	12/30/2016

FMCSA

System Name	Weakness Description	Status
FMCSA Motor Carrier Management Information Systems	The Incident Response plan does not define the time period required to report suspected security incidents to FMCSA in accordance with DOT and DHS CERT policy and procedures. *FMCSA reported the MCMIS system has been merged into FMCSA CE (Cloud Environment) as a subsystem. Therefore, the POAMs are managed under FMCSA CE. Due to quantity from the 2016 assessment, the FMCSA CE POAMs are managed outside of CSAM.*	After completion of the 2017 annual assessment for the FCMSA CE, all the appropriate POAMs will be entered or closed in CSAM by the 3PAO/ISSM as required. Assessment completion schedule for Nov 20, 2017.
FMCSA National Complaint Hotline Database	The reporting time periods in the Incident Response plan for reporting suspected security incidents have not been updated. The plan does not provide procedures for collecting metrics for measuring the incident response capability within the environment.	FMCSA reported after completion of the 2017 annual assessment for the NCHDB, all appropriate POAMs will be entered/managed in CSAM by the 3PAO/ISSM as required.

MARAD

System Name	Weakness Description	Status	Planned Finish Date
MARAD Maritime Service Compliance System	MARAD does not employ automated mechanisms to support the incident handling process.	Not found in CSAM	Not Specified
USMMA LAN	The Incident Response Plan has not been reviewed and approved annually.	Delayed	7/31/2016

OIG

System Name	Weakness Description	Status
OIG US DOT/OIG Infrastructure	The OIG Infrastructure does not incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises or implement the resulting changes accordingly as required by DOT policy. Security incident information is not reported to designated authorities as required by DOT policy.	In Progress. On 9/12/2017 OIG created a new POAM to address findings from 2016 that were not completed within DOT required timeframes. OIG reported they are on track for remediating these weaknesses by 2/1/2018.

OST

System Name	Weakness Description	Status	Planned Finish Date
Volpe Site Common Controls (VSCC)	There is no indication Volpe has reviewed the Incident Response plan at least annually, or as part of an after-action review. The record of changes indicates no revisions or reviews since the document was originally created. One of the individuals listed in the table of "Personnel List of Principles" is no longer part of the contractor work force.	Not Started	Not Specified

PHMSA

System Name	Weakness Description	Status	Planned Finish Date
PHMSA Safety Monitoring and Reporting Tool	SMART does not currently implement automated incident handling procedures. PHMSA reported these controls are inherited from the PHMSA portal system	Not found in CSAM	Not Specified

Source: OIG analysis

Exhibit H. OIG's Previous FISMA Reports

DOT Continues to Make Progress, But the Department's Information Security Posture Is Still Not Effective, (OIG Report Number FI2017008), November 09, 2016.

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.

Exhibit I. Open Recommendations from Previous FISMA Reports

Fiscal Year 2016, OIG Report Number FI-2017-008

Number	Recommendation
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. (STATUS: TO BE CLOSED)
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.

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, takes 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

Number	Recommendation
	and practices for effectively collecting, validating, and reporting ISCM data.
8	The Deputy Secretary, or his designees, takes 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, takes 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. (STATUS: TO BE CLOSED)
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.
15	Work with components to develop or revise their plans to effectively transition the remaining information systems to required 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

Number	Recommendation
	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 J. List of Acronyms

CIO	Chief Information Officer
COE	common operating environment
CSAM	Cybersecurity Assessment and Management System
CSM	configuration setting management
CSMC	Cyber Security Management Center
CVM	common vulnerability management
DOT	Department of Transportation
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FISMA	Federal Information Security and Management Act
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
ISCM	information security continuous monitoring
IT	information technology
MARAD	Maritime Administration
NHTSA	National Highway Traffic Safety Administration
NIST	National Institutes of Standards and Technology
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of the Secretary
PHMSA	Pipeline and Hazardous Materials Safety Administration
PIV	personal identify verification
POA&M	plan of action and milestones
US-CERT	United States Computer Emergency Readiness Team

Exhibit K. Major Contributors to This Report

KEVIN **DORSEY**	PROGRAM DIRECTOR
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

MEMORANDUM

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

SUBJECT: **ACTION**: Management Response to the OIG Draft Report—FISMA 2017: Project No. 17F3006F000

DATE: 12/20/2017

FROM: Kristen Baldwin
DOT Deputy Chief Information Officer

KRISTEN K. BALDWIN
Digitally signed by KRISTEN K. BALDWIN
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=KRISTEN K. BALDWIN
Date: 2017.12.20 17:32:09 -05'00'

TO: Calvin L. Scovel, III
Inspector General

The Department remains committed to improving its information security program and posture in defense of agency sensitive information, and interests. While we have made progress over the past year, the title of the OIG draft report does not adequately reflect the progress made and we request that the OIG reconsider the title. Each year since FY 2009, the DOT has increased the visibility of its cybersecurity program, risks, and threats; has improved its policy, processes, and integration with agency governance; and has invested in technology and capabilities to facilitate improved: detection of threats and risks; protection of agency information and systems; mitigation of risks; and recovery from incidents. During this past fiscal year, we have achieved several accomplishments to include the following:

- Developed and implemented an agency Cyber workforce management program and plan, and completed an initial assessment of agency cybersecurity personnel;
- Increased the percentage of properly authorized systems in the Office of the Secretary (OST) system inventory to above 90%;
- Initiated the DOT Network Assessment Risk Mitigation (NARM) initiative, in response to our FY 2016 network assessment, to completely redesign the non-FAA networks for future capabilities, improved performance, and improved security;
- Completed a transition from an agency Trusted Internet Connection (TIC) to commercial Managed Trusted Internet Protocol Services (MTIPS), with improvements to agency network resiliency, visibility into Internet activity, and the potential for lower future capital expenditures; and
- Implemented the DHS EINSTEIN 3 ACCELERATED (E3A) malicious e-mail filtering service to protect agency personnel from known-bad e-mail messages;

The DOT investment in cybersecurity will continue, with further maturation of capabilities aligned to the National Institutes of Standards and Technology's (NIST) Cybersecurity Framework, integration of cybersecurity into agency strategic planning, and exploitation of opportunities to improve cybersecurity through targeted investment in cloud and enterprise shared services.

Upon review of the OIG draft report we concur with recommendations 2, 4, 6, and 8 as written. We plan to implement recommendation 4 by February 1, 2018, recommendations 2 and 8 by October 1, 2018, and recommendation 6 by December 1, 2020.

We concur with recommendation 1 and propose an alternative action to require DOT components to follow and implement agency policy and processes, and only develop and implement their own policies and processes by exception, as approved by the DOT CIO. We plan to complete this action by October 1, 2018. We also concur with recommendation 7 and propose an alternative action to implement mandatory use of PIV or other agency-approved multi-factor authentication, except those instances that are subject to exclusions that are documented and approved. We plan to complete this action by December 1, 2019.

We concur in part with recommendation 3. The agency has already established policy and processes via the DOT Security Authorization and Continuous Monitoring Guide, as provided to OIG during this audit. We propose an alternative action to require that the common operating environment (COE) and FAA implement the Guide within their programs. We plan to complete this action by October 1, 2018.

We do not concur with recommendation 5 as this is a repeat finding for a prior recommendation that was closed by the OIG in March 2017. The same policies and processes, and updated data were provided to OIG for the FY 2017 audit.

We appreciate the opportunity to comment on OIG's draft report. If you have any questions, please contact me at 202-366-9201.

U.S. DOT OIG Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

https://www.oig.dot.gov/hotline

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590

www.oig.dot.gov