



U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

**FISMA 2018: DOT's Information Security
Program and Practices**

OST

Report No. FI2019023
March 20, 2019





FISMA 2018: DOT's Information Security Program and Practices

Required by Required by the Federal Information Security and Management Act of 2002

Office of the Secretary of Transportation | FI2019023 | March 20, 2019

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 471 information technology systems, which represent an annual investment of approximately \$3.6 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 cyber function areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

In all five function areas, DOT is at the Defined maturity level—the second lowest level in of maturity in the model for information security—because the Department has, for the most part, formalized and documented its policies, procedures, and strategies. However, DOT still has policy gaps. We found a number of instances in which implementation of processes did not conform to policy.

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

Our Recommendations

We made 12 recommendations to help the Department address challenges in its development of a mature and effective information security program. DOT concurred with all 12 of our recommendations.

Contents

Memorandum	1
Background	3
Results in Brief	6
Identify: DOT's Identify Function Controls Are Not Adequate	7
Protect: DOT's Protect Function Controls Are Not Adequate	18
Detect: DOT's Detect Function Controls Are Insufficient	23
Respond: DOT's Respond Controls Are Insufficient	25
Recover: DOT's Recover Function Controls Are Not Consistently Implemented	27
Conclusion	28
Recommendations	29
Agency Comments and OIG Response	30
Actions Required	30
Exhibit A. Scope and Methodology	31
Exhibit B. Organizations Visited or Contacted	36
Exhibit C. System Inventories for Fiscal Years 2017 and 2018, by OA	37
Exhibit D. Systems With Overdue Reauthorizations, by OA	38
Exhibit E. Systems With Weaknesses in Configuration Management, by OA	40
Exhibit F. System Weaknesses in User Identity Authentication and Access Management, by OA	49
Exhibit G. System Weaknesses in Data Protection and Privacy, by OA	56
Exhibit H. Weaknesses in Incident Response in Sample Systems, by OA	62
Exhibit I. OIG's Previous FISMA Reports	64
Exhibit J. Open Recommendations from Previous FISMA Reports	66


Exhibit K. List of Acronyms	69
Exhibit L. Major Contributors to This Report	70
Appendix. Agency Comments	71



Memorandum

Date: March 20, 2019

Subject: INFORMATION: FISMA 2018: DOT's Information Security Program and Practices | Report No. FI2019023

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 471 information technology (IT) systems, many of which are safety related and support transportation-related operations such as air traffic control. These systems represent an annual investment of approximately \$3.6 billion. Furthermore, 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 at DOT would protect these systems from disruptions of service and unauthorized, malicious access that could compromise safety operations or taxpayer dollars.

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 inspectors general to annually evaluate the effectiveness of these programs and report the results to the Office of Management and Budget (OMB).

For this year's review, OMB required inspectors general to assess 59 metrics in 5 security function areas—Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agencies' information security programs and the maturity level of each function area. OMB has defined five maturity levels³

¹ Pub. Law No. 107-347; 44 U.S.C. Chapter 35, Sub Chapter II, Information Security.

² The Federal Information Security Modernization Act of 2014 (Pub. Law No. 113-283) amends FISMA to, among other things, (1) reestablish the oversight authority of the Director of the Office of Management and Budget 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.

³ In *FY 2018 Inspector General FISMA Act of 2014 Reporting Metrics* (2018), OMB prescribes the metrics and provides the methodology to assess the maturity level of each function area.

as—from lowest to highest—Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

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, 2018. Specifically, we assessed DOT's performance in the five function areas.

We conducted our work in accordance with generally accepted Government auditing standards. To address OMB's 2018 FISMA reporting metrics, we assessed 48 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 details on our scope and methodology. As required, we provided our results to OMB via its web portal.⁴ 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

⁴ Because OMB designates this information For Official Use Only, we have not included our submission to OMB in this report.

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. Specifically, FISMA requires agencies to develop and maintain control techniques to address its requirements, including maintenance of an agencywide information security program. Furthermore, OMB regulations⁵ require Federal agencies to ensure that appropriate officials are assigned security responsibilities and periodically review their information systems' security controls. FISMA also requires agencies to report annually to OMB, Congress, and the Government Accountability Office (GAO) on the adequacy and effectiveness of their information security policies, procedures, and practices.

GAO's *Standards for Internal Control in the Federal Government* (Federal Control Standards)⁶ provides a framework for establishing and maintaining an effective internal control system. According to these standards, effective internal control requires oversight, an internal control mindset, and documentation of control activities, among things. In addition, the standards state that agency management designs appropriate control activities for the agency's information system and information technology infrastructure.

DOT's Operating Administrations (OA)—which for purposes of this report include the Office of the Secretary (OST) and the Office of the Inspector General (OIG)—manage the Department's 471 information systems. The majority of these systems (337 or 72 percent) are managed by the Federal Aviation Administration (FAA). The Saint Lawrence Seaway Development Corporation reported that it did have an information system that needed to be included in the inventory.

OMB and the Department of Homeland Security (DHS) annually issue FISMA guidance that includes the metrics OIGs are to use to evaluate agencies' information security programs. These metrics are based on the National Institute of Standards and Technology's (NIST) cybersecurity framework⁷ function areas—Identify, Protect, Detect, Respond, and Recover. See table 1 for the functions' definitions. 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 these metrics.⁸ The most significant change was the addition of a section on privacy that contains five new metrics.

⁵ OMB Circular A-130, *Managing Information as a Strategic Resource* (2016).

⁶ GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (2014).

⁷ NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (2018).

⁸ OMB and DHS, *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (2018).

Table 1. Definitions of Cybersecurity Framework Functions

Cybersecurity Framework Function	Definition	Number of metrics for each function
Identify	Requires agencies to develop the understanding needed to manage security risks to systems, assets, data, and capabilities. Includes metrics for risk management, security authorization, and weakness remediation.	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, data protection and privacy, and security training.	28
Detect	Requires agencies to develop and implement processes to identify incidents that may include security breaches. Includes metrics for information security continuous monitoring (ISCM).	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: OIG analysis of FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.

In the guidance, OMB and DHS also define a maturity model with five maturity levels used to assess the maturity and effectiveness of agencies' cybersecurity programs. The maturity levels are—from lowest to highest—Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Each inspector general also submits the assessment of his or her agency's performance in each function to OMB's web portal. Cyberscope, a tool at the web portal, then places the agency in one of the five maturity levels (see table 2). The inspector general also places his or her maturity assessment into the web portal for informational purposes. The foundational maturity levels ensure that agencies develop sound policies and procedures while the advanced levels capture the extent that agencies institutionalize those policies and procedures. OMB defines effectiveness as being Managed and Measurable in all function areas. However, an inspector general can reach a different conclusion based on agency's unique circumstances, and disclose that conclusion in Cyberscope.

Table 2. Definitions of Cybersecurity Maturity Levels

Maturity level (from lowest to highest)	Definition
Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Defined	Policies, procedures, and strategies 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 strategies and make necessary changes.
Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.

The Cyber Security Assessment and Management tool (CSAM) is DOT’s departmentwide system inventory, 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 17 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.

Results in Brief

The Department's cybersecurity program remains ineffective.

Overall and in each of the five function areas, DOT remains at the Defined maturity level. The Department has, for the most part, formalized and documented its policies and procedures in all function areas but still has some policy gaps. We also found a number of instances in which implementation of processes did not conform to policy.

In addition, we noted a number of internal controls that were not implemented because no law or regulation required the use of that specific control. This occurred in part because DOT officials erroneously addressed FISMA as a mandate to implement requirements instead of to build an internal control structure to effectively secure the Department's information systems.

Together, these policy gaps, implementation issues, and lack of understanding of internal control issues comprise significant deficiencies in security controls that increase the possibility that DOT's information or systems may suffer compromises that disrupt operations, impair safety, expose private data, or put tax dollars at risk. Examples of the more significant deficiencies in each function area follow.

1. **Identify.** The Cyber Security Assessment and Management tool (CSAM),⁹ DOT's main repository of departmental FISMA data, was not reliable. Furthermore, DOT was operating 61 systems with expired authorizations to operate and OAs authorized system operations with inadequate or no evidence of security controls assessments. We also found deficiencies in how DOT addressed weakness remediation, such as weaknesses that were not tracked in CSAM.
2. **Protect.** We found deficiencies in 30 of 48 sample systems pertaining to configuration settings, configuration change management, vulnerability scanning, and patch management. We also identified weaknesses in user identity authentication and specialized training. For example, over 211 systems were not set up to use multifactor user identity authentication.
3. **Detect.** DOT did not use standard data elements to maintain its inventories of hardware and software assets connected to its networks. The Department also had not defined the performance measures for its

⁹ A software that allows program officials and IT security managers to assess, document, manage, and report on the status of IT security risk assessments. It also provides a centralized system for the management of plans of action and milestones, including creation, tracking, and closing, and automates system inventory and FISMA reporting capabilities.

assessments of information security continuous monitoring (ISCM)¹⁰ program. Finally, DOT did not test security controls for the tools it used to support its ISCM/CDM program.

4. **Respond.** The Department had not addressed incident handling deficiencies we identified 2 years ago—the Cybersecurity Management Center’s (CSMC) lack of access to all DOT systems to monitor them for security incidents, and a ranking scheme to address incidents based on the seriousness of the risk they pose. DOT had also not resolved a number of incidents in a timely manner.
5. **Recover.** We found that all OAs had not implemented DOT’s contingency plans and testing requirements for at least one system. We also found that 36 sample systems did not meet OMB and FISMA requirements for contingency planning and testing. Based on our sample of 48 systems, we estimate that for 311 of 467 systems, or 66.5 percent,¹¹ the OAs did not perform effective contingency planning or testing.

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.

Identify: DOT’s Identify Function Controls Are Not Adequate

The Department has created policy for its Identify controls—which include metrics for risk management, security authorization, and weakness remediation—but gaps and implementation issues exist. Because the Department has not successfully maintained CSAM, it is not sufficiently reliable as a FISMA repository and oversight tool. The Department also has internal control weaknesses in system inventories, system authorization, system security testing, common control implementation, system deficiency resolution, and maintaining policy at the modal level.

¹⁰ A program collects information according to pre-established metrics, using information available through implemented security controls. ISCM maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

¹¹ Our 66.5 percent estimate has a margin of error of +/-14.0 percentage points at the 90 percent confidence level.

CSAM Is Not Reliable

In prior years, the Department had decided to expand the use of CSAM to improve its cybersecurity posture. However, we found multiple errors in the program—which we will discuss throughout this report—including

- an operational system listed as developmental,
- retired systems listed as operational,
- 138 contractor systems listed as Government systems,
- missing plans of actions and milestones (POA&M),
- missing artifacts—documents generated as part of security activities, such as security assessment reports,
- outdated artifacts, and
- missing data fields.

Several OAs informed us that we could not rely on the artifacts in CSAM for our audit purposes. In past audits, we used CSAM artifacts but were informed later that the artifacts were not correct. DOT has no process or control to validate CSAM's accuracy and completeness.

This lack of a reliable tool that centralizes security data makes it difficult for the Department to effectively oversee information security and assess risk.

OCIO Does Not Conduct Performance Oversight and Analysis Reviews of OAs Cybersecurity Programs

DOT policy¹² states that DOT's Chief Information Security Officer (CISO) should conduct program performance oversight and analysis of OAs' cybersecurity programs. These reviews should cover several aspects of FISMA, including whether systems (1) have authorizations, required security upgrades, and tested controls, (2) have the appropriate security impact levels, (3) have adequate and tested contingency plans, (4) conform to established baseline security configuration standards, and (5) have remediated their vulnerabilities.

An OCIO official informed us that his office did not conduct its annual program performance oversight and analysis reviews of OAs cybersecurity programs.

¹² DOT, *Security Authorization and Continuous Monitoring Performance Guide* (2018).

Instead of these analysis reviews, OCIO conducted integrated governance structured performance management reviews. As support for these reviews, we received

- examples of instances in which OAs submitted explanations of why systems were not authorized,
- copies of some risk acceptance memos, and
- sign-in sheets of some CISO meetings with OAs' information system security managers and directors to discuss FISMA audit expectations, OIG requests for information, and digital transformation.

This information did not provide evidence that OCIO's reviews covered the areas required for oversight and analysis reviews.

OCIO also provided information on to its reviews and approvals of OAs' IT Spend Plans, but this information has little bearing on assessments of the OAs' cybersecurity performance.

In a 2017 audit report, GAO noted that agencies should develop comprehensive security test and evaluation procedures and conduct examinations on a regular basis.¹³ GAO also noted that the agencies it reviewed performed reviews that were limited in scope—sometimes based on interviews and document reviews—and as a result, did not identify many of the security weaknesses that GAO found. DOT's lack of adequate and comprehensive performance reviews likely contributed to the recurrence of numerous weaknesses that we have identified and to its lack of awareness of these vulnerabilities. In-depth cybersecurity evaluations that examine security control effectiveness controls facilitate the identification of weakness that may place DOT at risk of compromise.

DOT Does Not Maintain a Comprehensive and Accurate Inventory of Its Information Systems

DHS and OMB require inspectors general to report on the extent to which their agencies maintain comprehensive and accurate inventories of their information systems, including cloud systems, third-party systems—systems that are contractor-operated—and “public facing” websites—those that allow public access. DOT policies and procedures state that the Department will maintain a comprehensive and accurate inventory of all information systems deemed reportable to OMB for FISMA.¹⁴ However, DOT's inventory does not include

¹³ GAO, *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities* (GAO-17-440T), February 14, 2017.

¹⁴ DOT's *FISMA Inventory Guide* (2013) defines a FISMA reportable system that any information system used by an OA that supports the conduct of DOT business and processes DOT information for, or on behalf of, the Department.

accurate counts of its cloud-based systems, contractor systems, or public facing websites.

We found that FAA and FRA did not correctly categorize 138 systems as contractor-operated in CSAM. FRA mislabeled 1 system and FAA mislabeled 137 systems as Government—or non-contractor—systems. FRA agreed to update its system categorization in CSAM. FAA and DOT's Chief Information Security Officer have developed new guidance on categorizing FAA's information systems, and the Department approved FAA's use of its own definition of contractor system. However, FAA's definition does not conform to OMB policy.¹⁵ DOT officials stated that the definition in OMB's policy is outdated. However, we found FAA's use of its own policy is likely to result in incorrect reporting of contractor systems. Improperly identified contractor systems make it difficult for DOT to ensure that it has sufficient controls over these systems.

Furthermore, the Department asserts that it has 68 cloud service providers but cannot link these to the FISMA reportable systems they support. The Department stated that it was planning to update CSAM with a capability for OAs to make these links. Currently to obtain this information, DOT officials would have to review individual system documentation.

DOT also did not provide an accurate inventory of its public facing websites to DHS in its June 2018 report.¹⁶ DHS scans the websites inventoried in these reports for vulnerabilities. DOT reported 617 public facing websites to DHS, but DHS found 92 additional websites. OAs had reported 17 of these 92 websites to the Department. When we asked about the discrepancy, the Department stated that the June 2018 report was a complete and accurate inventory of public facing websites. DOT's reporting process does not comply with the Federal Control Standards, which state that management should communicate quality information both internally and externally. DOT's lack of complete reporting to DHS creates a risk that the Department will not identify existing vulnerabilities. In addition, DHS noted that 50 percent of the DOT websites it scanned in June 2018 did not use secure protocols.¹⁷ The lack of secure protocol use makes the members of public that use these websites vulnerable to threats and loss of confidence in DOT services.

¹⁵ OMB Memorandum M-14-04 (2013).

¹⁶ A Cyber Hygiene report is the results of vulnerability scanning conducted by Department of Homeland Security's National Cybersecurity Assessments and Technical Services (NCATS) group. The purpose of the vulnerability scanning is to help secure agency internet-facing systems from weak configuration and known vulnerabilities.

¹⁷ OMB Memorandum M-15-13 (2015) requires all Federal websites to be compliant with the Hypertext Transfer Protocol Secure (HTTPS). HTTPS provides security by verifying a web site or service's identity and encrypting nearly all information sent between the website or service and the user.

The Department Operates Systems With Expired Authorizations

DOT operates systems that have expired authorizations. OMB requires¹⁸ each information system be authorized to operate by a senior agency official. This authorization ensures that all necessary security testing has been performed, weaknesses have been sufficiently identified and mitigated, and each system does not exceed risk tolerance.

Among the Department's 471 systems, we found 61¹⁹ that had expired authorizations to operate that belong to 6 OAs (see table 3).²⁰ According to DOT officials, these systems were not authorized for various reasons, including, among other things, (1) reauthorization was not a policy requirement, (2) some systems had been decommissioned, and (3) some systems had been restructured. However, we found no evidence of system decommissions or other activities.

The lack of system reauthorization inhibits executive decision making based on adequate and complete security testing to determine whether risks posed by a system is within the Agency's acceptable tolerance. See figure 1 for information on unauthorized systems since 2010.

Table 3. Numbers of Systems Overdue for Reauthorization as of June 2018, by OA

OA	Number of Systems
FAA	40
FMCSA	14
FTA	1
MARAD	1
NHTSA	4
OST	1
Total	61

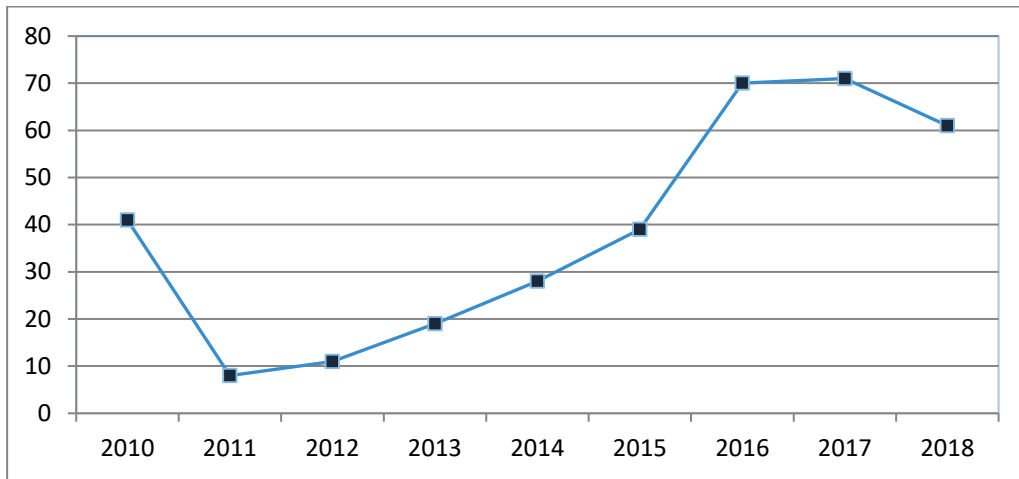
Source: CSAM and OIG analysis.

¹⁸ OMB Circular A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources* (2016).

¹⁹ In our 2017 review, we found 71 unauthorized systems.

²⁰ See exhibit D for a list of the 61 systems.

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



Source: OIG analysis of CSAM data

Some OAs Do Not Perform Adequate Testing of System Security Controls

Departmental policy²¹ requires OAs to annually assess the security controls for their information systems and operation environments. As a part of this assessment, OAs must develop security documentation that includes a security assessment plan, system security plan, and security assessment report.

For 22 of our 48 sample systems, the OAs authorized system operations with inadequate or no evidence of current security control assessments. We also found 23 sample systems that had inadequate system security plans and 47 whose system owners did not effectively monitor their systems' security controls. See table 4 for deficient systems by OA.

²¹ DOT-CA-2, *DOT Cybersecurity Compendium* (2018).

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

OA	Systems Tested	Inadequate Security Control Assessments	Inadequate System Security Plans	Inadequate Continuous Monitoring
FAA	28	18	17	27
FHWA	2	0	0	2
FMCSA	2	2	2	2
FRA	2	0	0	2
FTA	2	0	0	2
MARAD	2	1	1	2
NHTSA	2	1	2	2
OIG	2	0	0	2
OST	4	0	1	4
PHMSA	2	0	0	2
SLSDC*	0	0	0	0
Total	48	22	23	47

* SLSDC was not selected as part of the sample systems.
 Source: OIG analysis.

Based on our sample of 48 systems, we estimate that

- 213 of 467²² systems, or 45.6 percent,²³ were operating without adequate security control assessments,
- 210 of 467 systems, or 45.0 percent,²⁴ were operating without adequate system security plans, and
- 456 of 467 systems, or 97.6 percent,²⁵ were operating without adequate continuous monitoring of system specific or common controls.

This lack of adequate security plans, assessments and/or continuous monitoring, makes it difficult for authorizing officials to make effective decisions regarding the risk for compromise created by system operation.

²² During the sample selection process, we selected four systems reported as operational in CSAM that no longer existed. These errors in CSAM reduced the total number of systems to 467—not the 471 reported by CSAM. See exhibit A, Scope and Methodology, for our rationale.

²³ Our 45.6 percent estimate has a margin of error of +/-12.3 percentage points at the 90 percent confidence level.

²⁴ Our 45.0 percent estimate has a margin of error of +/-12.3 percentage points at the 90 percent confidence level.

²⁵ Our 97.6 percent estimate has a margin of error of +/-3.8 percentage points at the 90 percent confidence level.

DOT's Procedures for Monitoring Common Security Controls Are Insufficient

DOT lacks an effective process for OAs (excluding FAA) to assess, authorize, and monitor common security controls. A common control is one that supports multiple information systems. OMB requires²⁶ common control providers²⁷ to

1. document the controls in security plans,
2. conduct continual assessments of the controls' security, and monitor the controls' effectiveness, and
3. inform users when changes in the controls may adversely affect the protections the controls provide.

OST's Common Operating Environment²⁸ (COE) provides shared controls to most non-FAA systems. We found the following weaknesses in the implementation of the COE's common controls:

- OST did not perform assessments of the COE's security controls in 2015, 2016, or 2017, and accepted the risk;
- In June 2018, OST completed a security control assessment of the COE's security controls, but the assessor found deficiencies, including
 - continuous monitoring and software integrity controls that were not fully implemented in 2014 and 2018 assessments,
 - lack of timely installation of COE security patches,
 - lack of on-going COE security control assessments, and
 - lack of proper maintenance of system configuration baselines and settings.
- Although OST did not assess COE security controls for 3 years, and deficiencies were found in the 2018 assessment, none of the 10 OAs that use the COE's controls identified compensating or supplemental controls to implement, as required by DOT policy when common controls are not deployed.

²⁶ OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information System* (2013).

²⁷ The entity that has a system control used by another system.

²⁸ 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.

- Only PHMSA has a memorandum of understanding (MOU) with OST that delineates the responsibilities of each party regarding common controls' provision and use.
- Regular communication between authorizing officials and common control providers has not been established regarding the controls' security status and inherited risk.²⁹

OCIO officials stated that MOUs delineating responsibilities between OST and users of the COE's common controls are not required. OST officials also stated that DOT's policy, working capital funding agreements,³⁰ and the Federal Information Technology Acquisition and Reform Act of 2014 (FITARA)³¹ impact on DOT, and other factors, taken together, provide what MOUs can provide. As a result, MOUs are unnecessary. However, none of these documents delineates responsibilities as delineated in PHMSA's MOU with OST.

Regarding the lack of OAs' compensating controls, DOT officials stated that the COE's authorizing official had accepted all risks for the COE and the common controls it provided. According to DOT officials, this risk acceptance eliminates the requirement that users of the COE's common controls have compensating controls. The DOT officials stated further that because the COE provides the common controls, users of these controls are not required to perform security testing of these controls. While OST's authorizing official is responsible to authorize COE operation and test its controls' functionality, each system's authorizing official is responsible to ensure that his or her systems are operating within tolerable risks. For example, when an authorizing official reviews a new system's authorization package, he or she must consider the status of all the controls that protect it—both shared and not shared—to determine the overall risk to the organization based on the totality of control deficiencies and the system's impact.

According to Department officials, OAs' implementation of compensating controls (excluding FAA and OIG) is limited by FITARA. The officials stated that FITARA places a significant amount of IT spending under OCIO's control, and as a result, OAs that decide they need compensating controls may not be able to spend money on them because they lack approval or the controls may duplicate

²⁹ Inherited risks are those associated with security controls or portions of security controls controlled by another organization.

³⁰ The Working Capital Fund provides technical and administrative services that allow the Operating Administrations (OA) to focus on core missions while reducing costs by consolidating administrative management functions. The fund is sustained through negotiated agreements with its customers.

³¹ Title VIII, Subtitle D of the National Defense Authorization Act for Fiscal Year 2015, Pub. Law 113-291. FITARA outlines specific requirements related to, among other things, agency Chief Information Officer authority enhancements, enhanced transparency, and improved risk management in IT investments.

ones that the COE should provide.³² As a result, lack of suitable internal controls over the COE's common controls makes it difficult for the Department to ensure that systems operate at levels of tolerable risk.

Finally, the two OAs not impacted by FITARA—FAA and OIG—are taking steps to address compensating controls needed when common controls do not provide sufficient security. FAA officials informed us that one Agency line of business has implemented a program to assess the impact of compensating controls on its systems. OIG officials stated that the Agency plans to work with OST and the COE to develop a communication plan to get timely updates of testing results of common controls that OIG uses.

DOT's Security Weakness Remediation Process Lacks Adequate Controls

FISMA requires agencies to develop processes to remediate security weaknesses that they detect during system monitoring and testing. OMB³³ requires agencies to develop POA&Ms with remediation start dates for these weaknesses, and to prioritize weakness remediation based on the seriousness of each weakness. Furthermore, DOT policy³⁴ 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 9,793 open POA&Ms—an increase of 5,264 (116 percent) from 2017's 4,529—some of which date from 2009 (see table 5). We also found that

- 1,790 POA&Ms, including 309 high priorities and 1,481 medium priorities, with remediation start dates marked "to be determined," indicating that the OAs had not begun work to resolve the weaknesses, and
- 1,365 POA&Ms, including 193 high priorities and 1,172 medium priorities, did not have documented remediation costs.

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.

³² In July 2017, the Department issued an IT Shared Services Memo that requires OAs to consolidate utility IT services such as cloud computing, storage, telecommunication and backup/recovery under OST's COE, the common control/service provider for these utility IT services.

³³ OMB Memorandum M-03-19, *Reporting Instructions for FISMA and Updated Guidance on Quarterly IT Security Requirements* (2003).

³⁴ DOT Order 1351.37; DOT, *Security Weakness Management Guide* (2017).

Table 5. Summary of POA&Ms Opened Between 2009 and 2018 Without Start Dates or Documented Remediation Costs, by OA

OA	Open POA&Ms	Actual start dates marked as "TBD"	No documented cost
FAA	8021	1376	1004
FHWA	41	0	0
FMCSA	726	93	93
FRA	90	44	0
FTA	37	0	0
MARAD	440	121	118
NHTSA	24	18	9
OIG	10	8	8
OST	373	130	133
PHMSA	31	0	0
SLSDC	0	0	0
Total	9793	1790	1365

Source: CSAM POA&M report dated July 2018.

We found that a large number of the 9,793 open POA&Ms belonged to FAA. FAA officials informed us that the Agency is addressing past OIG recommendations by updating in CSAM its POA&Ms for 128 information systems, and will complete this process by the end of the 2018 calendar year. Previously, FAA did not include its POA&Ms in CSAM. FAA's inclusion of its POA&Ms in CSAM is a step in the right direction, but the Agency's high numbers of POA&Ms illustrate the degree of inaccuracy that has existed in CSAM for years.

Furthermore, the information on POA&Ms in CSAM for our sample systems was incomplete. We found that for 39 of 48 sample systems, the OAs had not submitted to CSAM POA&Ms on all identified security weaknesses. Based on our sample of 48 systems, we estimate that 404 of 467 systems, or 86.6 percent,³⁵ have system specific security weaknesses that are not reported and managed in CSAM.

OCIO stated that OAs are not required to disclose actual start dates and remediation costs in CSAM, but under DOT policy they are mandatory. The lack of this information in CSAM inhibits OCIO's ability to use CSAM to determine whether OAs have begun remediation, estimated costs, and properly completed POA&Ms. Incomplete POA&Ms inhibit the Department's ability to assess risk and

³⁵ Our 86.6 percent estimate has a margin of error of +/-3.9 percentage points at the 90 percent confidence level.

funding requirements, analyze weakness trends, determine whether actions have been taken, and implement departmentwide solutions.

Four OAs Have Not Developed their Own Risk Management Policies and Procedures

Four OAs—MARAD, NHTSA, OST, and SLSDC—did not provide copies of their risk management policies and procedures, and stated that they follow the Department’s policy. However, DOT’s Cybersecurity Compendium³⁶ states that each OA must develop, disseminate, review, and annually update risk management policies and procedures that include appropriate elements such as criteria for making risk based decisions. The Federal Control Standards state that management is responsible for designing policies and procedures to fit the agency’s circumstances. A lack of policies and procedures that address how OAs assesses risks puts the OAs’ and the Department’s information systems at risk of compromise.

Protect: DOT’s Protect Function Controls Are Not Adequate

DOT’s Protect controls—which cover configuration management, user identity authentication and access management, data protection and privacy, and security training—are inadequate. Furthermore, lack of clarity in the Department’s specialized training policy decreased the likelihood that all who required this training received it.

DOT's Controls Over Configuration Management Are Inadequate

OCIO does not enforce OMB’s requirements³⁷ for addressing weaknesses in configuration management.³⁸ We found weaknesses in 30 of 48 sample systems pertaining to configuration settings, change management, vulnerability scanning,

³⁶ DOT, OST, OCIO, *Departmental Cybersecurity Compendium Supplement to DOT Order 1351.37 Departmental Cybersecurity Policy*, (2018)

³⁷ OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (2013).

³⁸ Configuration management entails a set of activities to establish and maintain system and component integrity through control of initializing, changing, and monitoring the configurations of those systems and components.

and patch management (see exhibit E). Some of these weaknesses lacked scheduled completion dates for remediation.

For example, for its Comprehensive Academic Management System (CAMS), MARAD completed its last security control assessment in 2015. POA&Ms for weaknesses identified during this assessment have no scheduled completion dates. CAMS also contains a substantial amount of personally identifiable information (PII), including social security numbers, credit card numbers, and health information. At the time of our review, MARAD had not conducted a privacy impact assessment³⁹ of CAMs. OMB requires these assessments for all information systems that contain substantial PII.

Unresolved weaknesses in configuration management make it difficult for DOT to ensure its information systems are adequately secured and protected and put the systems at risk for compromise.

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

OMB required that, by 2012, all Federal employees and contractors use personal identity verification (PIV) cards to login to agency computers and to access system applications. The 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 policy⁴⁰ requires PIV cards as the primary means of identification and authentication for access to its information systems. OMB⁴¹ also requires 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 September 12, 2018, 150 of 468⁴² systems reported in CSAM required PIV cards for user identity authentication. However, many DOT systems do not comply with this requirement. Specifically, we found that

- 211 systems were not enabled for PIV card use, and 34 were unspecified, meaning there was no indication whether the system could use PIV cards,

³⁹ A privacy impact assessment determines whether a system creates a risk to the privacy of the individual that owns the PII.

⁴⁰ DOT Cybersecurity Compendium.

⁴¹ OMB Memorandum M-11-11, *Policy for a Common Identification Standard for Federal Employees and Contractors* (2011).

⁴² As of September 2018, the Department reported 468 systems in CSAM.

- 73 systems were enabled for PIV access but did not require users to use PIV cards for access, allowing users to employ less secure means for identity authentication such as usernames and password, and
- 54 of 197 systems containing PII were not PIV enabled for identity authentication.

We also found that 29 of 48 sample systems have weaknesses in user identity authentication and access management (see exhibit F) were either not documented in CSAM or had passed or were approaching their remediation dates.

In addition, DOT has not fully implemented use of PIV cards for use of virtual desktop infrastructure⁴³ (VDI) for remote access, a weakness we identified in 2016, or for physical access to all of its facilities. As of September 12, 2018, FAA had enabled 194 of its 510 facilities for PIV access. FAA plans to complete PIV implementation at the remaining facilities by the end of fiscal year 2019.

The lack of 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 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 Have Not Met All Data Protection and Privacy Requirements

For this year's review, OMB's reporting metrics require inspectors generals to assess their agencies' data protection and privacy programs. DOT has established policies and responsibilities for managing privacy risk in the creation, collection, maintenance, use, storage, transmission, protection and destruction of PII.

However, in our 48 sample systems, we found security and privacy weaknesses in 24 sample systems designated as PII systems. See exhibit G for a list of these weaknesses.

For example, OST had not implemented use of tools to check software integrity for the COE. OST also had not established procedures for notifications of failures in integrity verification. The COE does not respond automatically when integrity violations are discovered, and OST has no tools to help detect changes to the COE. Furthermore, once they are discovered, these violations are not correctly reported as security incidents.

⁴³ VDI enables a user to have a DOT server remotely replicate his or her desktop on devices.

We also found that 20 of 48 sample systems at 6 OAs—FAA, FRA, MARAD, NHTSA, OST, PHMSA—did not have completed privacy threshold analyses (PTA). A PTA determines what privacy risk management activities—such as a privacy impact analysis—must be completed to ensure that initiatives do not create undue privacy risks for individuals that own PII.

The majority of the Department’s privacy risk emanates from the collection, use, storage, and sharing of PII, and the IT systems used to support these processes. As a result, the lack of privacy protection puts the PII stored in DOT’s information systems at risk for compromise.

DOT Nearly Met Its Security Awareness Training Goals

FISMA requires agencies to develop and maintain security training programs 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 require⁴⁴ agencies to provide security awareness training to all employees and contractors, even those that never access computer systems.

Departmental policy⁴⁵ required the OAs to ensure that by August 31, 2018, 95 percent of their personnel completed security awareness training for fiscal year 2018. The Department came close to meeting this requirement. Overall, 93 percent of departmental personnel completed security training. Specifically,

- FHWA, FMCSA, FRA, FTA, MARAD, NHTSA, PHMSA and SLSDC exceeded the 95 percent goal, and
- while FAA, OIG, and OST did not meet the goal, all three did train over 90 percent of their personnel.

Meeting security training goals decreases the possibility that employees will engage in activities that could lead to security compromises. DOT still has some security awareness training deficiencies. For example, the Department did not provide documentary evidence that it has a defined process to tailor its training for its unique missions and to obtain feedback to evaluate and improve its program. Tailoring for unique missions and using feedback can help improve a training program to better prepare users to avoid cybersecurity compromises.

⁴⁴ OMB Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (2007).

⁴⁵ DOT, *Cybersecurity Action Memo 2018-001, FY18 Mandatory Security Awareness Training Implementation Guidance* (2018).

DOT's Policy on Specialized Training Is Unclear

FISMA requires agencies to develop and maintain security training programs to ensure employees with information technology or security related duties receive the appropriate specialized security training. While DOT's training policy is generally at the Defined maturity level, we identified a deficiency in its specialized training policy. OCIO issued specialized training policy in 2018⁴⁶ that conflicts with the Department's Cybersecurity Compendium policy. We found that:

- OCIO policy requires only four positions—Security Control Assessor, Cyber Defense Incident Responder, Cybersecurity Operations Specialist, and Security Analyst—to complete specialized training. Other positions such as CIOs, information security officers, and IT auditors, were not required to have specialized training. The Compendium requires OAs to identify all personnel and contractors with significant security roles.
- The Compendium requires the Department's Chief Information Security Officer to specify the minimum hours of specialized security training required annually, and OAs to ensure these hours are met. However, the OCIO's policy states that training should be based on courses that map to competencies instead of hours. As a result of this contradiction, most OAs did not provide hours of training for personnel that received specialized training. Without a minimum hourly requirement, we could not determine whether employees met requirements.
- Some OAs provided training to personnel in addition to the four positions stated in OCIO policy. However, the lack of a comprehensive list of positions inhibits DOT's ability to ensure that all personnel that require specialized security training receive it.

A lack of clearly defined policies, procedures, guidance, and instructions from OCIO to the OAs regarding annual specialized training for personnel with security related duties makes it difficult for DOT to be sure that its personnel have the knowledge, skills, and abilities to protect the Department's information systems.

⁴⁶ DOT, Cybersecurity Action Memo 2018-002, *FY18 DOT FY18 Specialized Cybersecurity Training Implementation Guidance* (2018).

Detect: DOT's Detect Function Controls Are Insufficient

The Department's Detect controls—which cover information security continuous monitoring (ISCM)—are not sufficient. DOT lacks a reliable inventory of the hardware and software assets it has to monitor, and has not clearly defined qualitative and quantitative performance measures for its ISCM program. Furthermore, the Department and FAA lack rigorous ISCM programs.

DOT Has Not Provided Clear Guidance for the OAs on Hardware and Software Inventories

NIST standards⁴⁷ and DOT policy require OAs to develop and document comprehensive hardware and software inventories, and to update these inventories as installations, removals, and software updates occur. The OAs must also provide quarterly updates to OCIO on their current inventories. OCIO then reports to OMB.

However, OCIO has not provided the OAs with clear guidance on what data they must provide to OCIO. Specifically, OCIO has not defined the content, data fields, or taxonomy that make up the inventory or a process for developing and maintaining up-to-date inventories with information sufficiently detailed for tracking and reporting. We found that some OAs use internal policies and/or outdated departmental policies⁴⁸ to manage their inventories.

This lack of clear guidance has resulted in inconsistencies in the information that OCIO and OAs report. OCIO reported approximately 159,000 hardware assets for the fiscal year 2018 third quarter to OMB. However, the OAs reported to us approximately 77,000 in hardware assets, a difference of 82,000. Only 3 OAs provided some form of a software inventory. OCIO provided a data dump that listed the software that runs on the COE, according to BigFix. However, the information was missing data fields needed for verification.

⁴⁷ NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (2011).

⁴⁸ Some OAs stated that they continue to use outdated and/or rescinded, such as *DOT Automated Enterprise Continuous Monitoring System Guide* (2013).

DOT Has Not Properly Developed Cybersecurity Performance Measures

NIST guidance describes the process to develop performance measures and states that a key consideration are selecting measures most appropriate for an agency's strategy and business environment, including mission and information security priorities, environment, and requirements.

OCIO officials informed us that they had adopted OMB's Federal Government CIO FISMA metrics,⁴⁹ and that DOT's Security Authorization and Continuous Monitoring Performance Guide identified ISCM performance measures. However, OMB's metrics are not designed specifically for DOT's business environment, and DOT's Guide does not identify any process to develop such measures. As a result, DOT is operating without properly developed Department-specific cybersecurity performance measures. The lack of these measures inhibits the Department's ability to monitor progress, identify areas that need attention and determine the effectiveness of its cybersecurity program, including ISCM.

DOT's and FAA's ISCM and CDM Programs Are Deficient

DOT and FAA's ISCM and continuous diagnostics and mitigation (CDM) programs have deficiencies that limit the effectiveness of their monitoring of IT assets. DHS works with Federal agencies to plan and integrate tools and services to automate the monitoring and assessment of risk. DOT and FAA's ISCM/CDM programs include these capabilities. They both use the software tool BigFix⁵⁰ for continuous asset monitoring.

According to CSAM, the Department's ISCM/CDM program is in its developmental phase, even though BigFix is currently operating. For example, when preparing hardware and software inventories, DOT uses BigFix. However, BigFix does not have a system authorization. DOT officials informed us that they were waiting to obtain other components of the CDM program to authorize them along with BigFix as a group. This lack of system authorization makes it difficult for DOT to be sure it is fully aware of the risks that BigFix poses to the

⁴⁹ OMB issues FISMA metrics for CIOs that focus on assessing agencies' by ensuring agencies implement the Administration's priorities and best practices; and providing OMB with the performance data to monitor agencies' progress toward implementing the Administration's priorities.

⁵⁰ The CDM/BigFix 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.

Department, and that it has the necessary controls in place to ensure its proper operation.

Furthermore, according to CSAM, FAA's ISCM and CDM program is in the implementation phase. FAA reported that the Agency is making progress with the implementation of its ISCM program. However, FAA also acknowledged that the Agency is not yet ready to declare its systems ready for ongoing authorization because its current ISCM program does not monitor all security controls with the appropriate degree of rigor and at the frequencies envisioned by its ISCM strategy. In addition, during our recent audit of DOT's ISCM,⁵¹ FAA officials stated that the Agency had not completed phase 1 of the CDM process. FAA officials stated further that the Agency's implementation of CDM's for the National Airspace System (NAS) may be limited due to air traffic and safety concerns. For example, FAA would need to be sure that putting a CDM tool on a safety related system would not inadvertently provoke a system disruption.

This lack of a comprehensive information security monitoring program inhibits the Department's ability to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Respond: DOT's Respond Controls Are Insufficient

DOT's Respond controls, which address incident response, are insufficient. According to DOT policy,⁵² when an incident such as a security breach or interruption of service occurs, the OA must report the incident to the Department's Cybersecurity Management Center (CSMC). CSMC analyzes the incident, categorizes it, and reports it to United States Computer Emergency Readiness Team (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 OAs by contractors and other Government organizations. The Department's established policies, procedures, and processes governing incident response are characteristic of a program at a defined level of maturity.

At FAA and OIG, we found 10 unresolved incidents that were over 90 days old (see table 6), all of which occurred in 2017. Three of the incidents were confirmed breaches related to PII. One included medical records mailed to the wrong address.

⁵¹ DOT Has Not Met Federal Targets for Implementing Components of Its Information Security Continuous Monitoring Program (OIG Report No. F12019014) December 4, 2018.

⁵² OCIO, *Cyber Security Incident Response Plan* (2014).

Table 6. Unresolved Incidents Over 90 Days Old

No.	Age	Incident Title	Incident Description	Open Date	Last updated
1	358	PII Incident	Medical records mailed to the wrong address **	8/10/17	8/22/2017
2	358	PII Incident	Potential PII data found on KSN SharePoint site	8/29/17	8/31/2017
3	357	Vulnerability	NCCIC NCATS Cyber vulnerability	9/25/17	9/25/2017
4	350	PII Incident	Release of PII Data **	9/27/17	9/28/2017
5	345	Vulnerability	NCCIC NCATS Cyber vulnerability.	10/3/17	10/3/2017
6	343	Vulnerability	NCCIC NCATS Cyber vulnerability	10/3/17	10/3/2017
7	342	Potential PII	Email address spillage	10/18/17	10/21/2017
8	338	Vulnerability	NCCIC NCATS Cyber vulnerability	11/2/17	11/2/2017
9	324	Vulnerability	NCCIC NCATS Cyber vulnerability	11/15/17	11/15/2017
10	322	PII Incident	Privacy breach in the UAS pilot system **	12/11/17	12/14/2017

* Open incident data retrieved on August 7, 2018.

** Confirmed breach.

Source: OIG analysis of DOT data.

We also found that some OAs did not comply with all FISMA and DOT requirements regarding incident response. Specifically, we found 20 security incident-related weaknesses in 10 of 48 sample systems that have not been remediated on schedule (see exhibit H).

The Department has also not implemented recommendations we made in 2016⁵³ to resolve issues at CSMC. CSMC continues to lack access to all departmental systems and network maps, and a ranking scheme to address incidents based on the seriousness of the risk they pose. For example, FAA’s Security Operations Center does not have a network mapping of the NAS’s information systems to ensure FAA has visibility into all NAS incidents. FAA’s Security Operations Center obtains information on the status of NAS incidents from the NAS Operations Center and then submits the information to CSMC.

CSMC’s inability to monitor all DOT systems creates the risk that not all incidents get reported to US-CERT. As a result, DOT and US-CERT cannot be sure that they can mitigate 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.

⁵³ DOT Cybersecurity Incident Handling and Reporting Is Ineffective and Incomplete (OIG Report No. FI2017001), October 13, 2016.

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

While DOT's Recover controls for contingency planning are not fully implemented at all 10 OAs tested,⁵⁴ they are at a Defined maturity level because DOT has, for the most part, formalized policy and procedures for this function. DOT policy⁵⁵ requires agencies to establish and periodically test contingency plans⁵⁶ for continuation of operations and services, including those provided by information systems, in the event of an emergency shut down. DOT policy also requires that agencies test and update their contingency plans at least annually.

Among our 48 sample systems, we found that the 10 OAs tested had not implemented DOT's contingency plans and testing requirements for at least 1 system. We also found that 36 sample systems did not meet OMB and FISMA requirements for contingency planning and testing. For example,

- FMSCA has not developed a contingency plan for the FMCSA Service Center System since 2012,
- MARAD has not performed a contingency plan test on CAMS since 2007,
- OST has not conducted a test at the COE's current disaster recovery facility, and
- FAA Mike Monroney Aeronautical Center Trusted Internet Connection did not perform a functional contingency plan test.

Based on our 48 sample systems, we estimate that for 311 of 467 systems, or 66.5 percent,⁵⁷ the OAs did not perform effective contingency planning or testing.

We also found that

- FAA, FMCSA, OIG, FTA, MARAD, NHTSA, and PHMSA did not define roles and responsibilities for stakeholders in contingency planning for some of its systems;

⁵⁴ SLSDC did not have a sample system selected for this year's FISMA review. However, during our review we identified an SLSDC system that may be FISMA reportable.

⁵⁵ DOT Cybersecurity Compendium (2018).

⁵⁶ A contingency plan contains policy and procedures for an agency's response to a loss of mission capability and is used by risk managers to determine what happened and 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 failure or destruction of facilities. A business continuity plan documents a predetermined set of instructions or procedures for how an agency will sustain mission and business functions during and after a disruption.

⁵⁷ Our 66.5 percent estimate has a margin of error of +/- 14.0 percentage points at the 90 percent confidence level.

- FRA, MARAD, NHTSA, and OST did not define and implement contingency planning policies, procedures, and strategies as required, and that FMCSA, OIG, and FTA did not annually update their policies per DOT policy;
- FAA did not provide evidence of a business impact analysis⁵⁸ for 16 systems, and MARAD did not do so for 1 system. FAA, FRA, FMCSA, FTA, NHTSA, MARAD, OIG, and PHMSA did not provide evidence that they had incorporated business impact analyses into some of their systems' continuity of operations plans, business continuity plans, and disaster recovery plans;
- FAA, FMCSA, FRA, FTA, MARAD, NHTSA, OIG, and PHMSA did not ensure that their Information system contingency plans were developed, maintained, and integrated with other continuity plans;
- FAA, FMCSA, FRA, FTA, MARAD, NHTSA, OST, and PHMSA did not conduct annual contingency plan testing and exercises for all their systems as required;
- FAA, FMCSA, FRA, MARAD, NHTSA, and PHMSA did not identify alternative sites to perform information system backup and storage as appropriate; and
- only two OAs—FHWA and FTA—communicated to stakeholders information on planning and performance of recovery activities for their information systems.

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, and handling billions of dollars. DOT's cyber security program must protect these systems from malicious attacks and other compromises that may put citizen safety or taxpayer dollars at risk. While DOT continues update its policies and procedures, and maintain a defined level of maturity, we continue to find persistent deficiencies in the implementation of the policy and processes that create an effective information security program. The effect of these deficiencies is exacerbated by the Department's growing

⁵⁸ A Business Impact Analysis helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes.

“compliance” mindset and non-implementation of controls it believes are not required by law or regulation. These deficiencies place DOT’s information systems at an increased risk of compromise and make them a 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. Develop policy and procedures to verify and validate the accuracy and completeness of the Department’s key FISMA information repository and tool, currently the Cyber Security Assessment and Management tool (CSAM).
2. Direct OCIO to follow policy and conduct annual cybersecurity performance analysis reviews of OAs’ cybersecurity programs, and submit reports to OAs with recommendations to address cybersecurity weaknesses.
3. Develop a process and policy where applicable to ensure the Department develops and maintain a comprehensive and accurate inventory of cloud systems, contractor systems, and websites that the public can access.
4. Direct OST to prioritize and resolve COE security weaknesses identified by assessor, and develop POA&Ms that realistically reflect resources and timeframes for completions of these actions
5. Direct OST to establish MOUs that delineate the responsibilities for COE common controls with each of the following OAs: FHWA, FMCSA, FRA, FTA, OIG, MARAD, SLSDC, and NHTSA.
6. Direct OAs (FAA, FHWA, FMCSA, FRA, FTA, OST, PHMSA, MARAD, and NHTSA) with weaknesses in data protection and privacy to update the status and develop POA&Ms to address the weaknesses.
7. Update specialized training guidance in DOT Cybersecurity Action Memos policy and DOT Cybersecurity Compendium policy to clearly define requirements.
8. Enhance security awareness training policy to define processes to tailor this training to DOT’s unique environment and use feedback to enhance its program.

9. Develop and define a taxonomy that describes the content of the hardware and software inventory and the process to assemble, verify and maintain adequate support for the inventory data as well as the related information reported to OMB and other external parties.
10. Develop a process to define its performance measures—that consider DOT's business environment—to assess the effectiveness of DOT's information security program, including its ISCM program,
11. Using NIST guidance, test and authorize CDM applications (such as BigFix) that have been placed into operation on DOT's networks without proper security control assessments.
12. Provide enterprise wide specialized training on contingency planning and testing on a periodic basis to appropriate security officials and stakeholders. Training should reinforce crucial role contingency planning and testing plays in an effective information security program.

Agency Comments and OIG Response

We provided DOT with our draft report on December 07, 2018, and the department requested an extension to provide their response on January 25, 2019. Due to the government shutdown, the department's response to our audit report was delayed. OIG received its formal response on March 01, 2019. DOT's response is included in its entirety as an appendix to this report. DOT has concurred with all 12 of our recommendations and proposed appropriate actions and completion dates.

In its response, the Department notes that, by the end of fiscal year 2018, it received a higher overall rating of "Managing Risk" under DHS's risk management assessment (RMA) methodology. While this is a positive result, it is important to note that DHS uses unaudited data submitted by the Department in order to determine its ratings.

Actions Required

We consider recommendations 1 through 12 resolved but open pending completion of planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between February and December 2018, 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, 2017, and June 29, 2018. 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 29, 2018. We obtained a universe with 471 systems from CSAM repository the Department uses to track system inventories, weaknesses, and other security information. We divided this universe into 14 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 and a maximum of ten in order to meet our statutory reporting deadline. We selected a stratified simple random sample of 48 out of 471 computer systems. During our audit we found that two systems in our universe were merged with existing systems, one was retired, and one system was created in error, so that we reviewed a stratified sample of 48 out of 467 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 +/-14.0 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-1. OIG’s Representative Subset of Sample Systems by OA

FAA

	System	Impact Level a	Contractor System b
1	FAA Continuous Diagnostics and Mitigation	High	No
2	Mike Monroney Aeronautical Center Trusted Internet Connection	High	No
3	AIT Databases	High	No
4	APL Singapore LAN	Moderate	No
5	Enterprise Architecture and Solutions Environment	Moderate	Yes
6	Designee Management System	Moderate	No
7	NACIP (National Automated Conformity Inspection Process)	Moderate	No
8	Federal Aviation Administration Directory Services	Moderate	No
9	Direct User Access Terminal II CSC	Moderate	Yes
10	WMSCR (Weather Messaging Switching Center Replacement Sustainment)	Moderate	No
11	ASDE-X (Airport Surface Detection Equipment - Model X)	Moderate	No
12	AMASS (Airport Movement Area Safety System)	Moderate	No
13	TDWR (Terminal Doppler Weather Radar)	Moderate	No
14	Wind Hazard Detection Equipment	Moderate	Yes
15	ARSR 1/2 (Air Route Surveillance Radar Models 1 & 2)	Moderate	No
16	SWIM Terminal Data Distribution System	Moderate	No
17	VRRP/DALR (Voice Recorder Replacement Program/Digital Audio Legal Recorder)	Moderate	No
18	IVSR (Interim Voice Switch Replacement System)	Moderate	No
19	Information Technology Asset Management System	Low	No
20	Hazard Identification, Risk Management & Tracking	Low	No
21	ADAS (Automated Weather Observation System Data Acquisition System)	Low	No
22	Parsons Data System	Low	No
23	CPDS (Critical Power Distribution System)	Low	No
24	Airports Geographic Information System	Low	Yes
25	FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System	Low	Yes
26	Instrument Flight Procedures Automation-Mission Support	Low	No

	System	Impact Level a	Contractor System b
27	Real Property Financial Management Tool (RPFMT)	Low	No
28	Building Automation System	Low	No

FHWA

	System	Impact Level ^a	Contractor System ^b
1	User Profile and Access Control System	Moderate	Yes
2	Freedom of Information Action System	Moderate	Yes

FMCSA

	System	Impact Level ^a	Contractor System ^b
1	FMCSA Service Center	Moderate	No
2	SafetyNet	Moderate	Yes

FRA

	System	Impact Level ^a	Contractor System ^b
1	FRA Hosting and Operation Support Technology Service (FRA-HOSTS)	Moderate	No
2	Railroad Enforcement System	Moderate	No

FTA

	System	Impact Level ^a	Contractor System ^b
1	FTA General Support System (FTA GSS)	Moderate	Yes
2	Appian	Moderate	Yes

MARAD

	System	Impact Level ^a	Contractor System ^b
1	MARAD Internet	Moderate	Yes
2	Comprehensive Academic Management System (CAMS)	Moderate	Yes

NHTSA

	System	Impact Level ^a	Contractor System ^b
1	NHTSA119: Grants Management Solutions Suite	Moderate	Yes
2	NHTSA009: Fatality Analysis Reporting System	Moderate	Yes

OIG

	System	Impact Level ^a	Contractor System ^b
1	Computer Crimes Unit Network	Moderate	No
2	JA-20 Lab	Moderate	No

OST

	System	Impact Level ^a	Contractor System ^b
1	Common Operating Environment (COE)	High	Yes
2	Parking and Transit Benefit System (PTBS)	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	PHMSA Portal System	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

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 2017 and 2018, by OA

OA	Fiscal Year 2017	Fiscal Year 2018	Change
FAA	323	337	14
FHWA	16	18	2
FMCSA	19	19	none
FRA	12	11	(1)
FTA	8	8	none
MARAD	15	15	none
NHTSA	17	19	2
OIG	2	3	1
OST	44	34	(10)
PHMSA	7	7	none
SLSDC	1	0	(1)
Total Systems	464	471	7

Sources: CSAM as of February 2, 2018, and OIG analysis

Exhibit D. Systems With Overdue Reauthorizations, by OA

OA	Asset	Total
FAA	Aviation Camera System	40
	Alaska Region Facility Security System	
	Enhanced Terminal Voice Switch	
	Surveillance and Broadcast Services Monitor	
	Tower Data Link Service	
	Central Altitude Reservation Function	
	Comprehensive Management Resource Information System	
	FDP 200	
	Flight Activity and Crew Tracking System	
	Integrated Communications Switching System	
	Weather and Radar Processor	
	National Airspace system Aeronautical management Enterprise System	
	Time Based Flow Management	
	Integrated Control and Monitoring System	
	Building Access, Software and Hardware for MMAC	
	AOV Facility Specific Safety Standard	
	International Aviation Standards Data Exchange	
	Aviation Safety Hotline Information System	
	APL Singapore LAN	
	AST LAN	
	ATO EDC MMAC	
	ATO Network	
	AWA Hangar 6 LAN	
	Brussels LAN	
	WJHTC Enterprise Data Center	
	WJHTC LAN	
	ARC LANS	
	Information Resource Management System	
	ARP LANS	
	Data Communication Trial Automation Platform	
	Direct User Access Terminal/ Data Transformation Corporation	
	AVS LAN/WAN	
Enhanced Inventory Logistics and Maintenance System		
Mike Monroney Aeronautical Center Voice		

OA	Asset	Total
	Alaska Boundary Connection	
	NAS Data Warehouse	
	Simulator Inventory & Evaluation Scheduling System	
	FAA Transit Benefits	
	Information Technology Asset Management System	
	En Route Information Display System	
FMCSA	CDLIS-Gateway	14
	FMCSA Cloud Environment	
	A&I-NCCDB Data Qs	
	Electronic Document Management System	
	FMCSA Portal	
	Licensing & Insurance	
	Motor Carrier Management Information Systems (MCMIS)a	
	National Registry of Certified Medical Examiners System, SAFETYNET	
	Performance and Registration Information Systems Management	
	Query Central	
	Safety and Fitness Electronic Records	
	FMCSA Service Center	
	Enforcement Management Information System	
FTA	Appian	1
MARAD	Common Content Environment (CCE)	1
NHTSA	NHTSA Inventory System	4
	National Sobriety Testing Resource Center (NSTRC)	
	Crash Test Databases	
	Traffic Records Improvement Program Reporting System (TRIPS)	
OST	Correspondence Control Management System	1
Total		61

Source: CSAM as of February 2, 2018, and OIG analysis

Exhibit E. Systems With Weaknesses in Configuration Management, by OA

FAA

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
Continuous Diagnostics and Mitigation	CDM subcomponents do not develop, document and maintain current baseline configurations.	Delayed	9/30/2017
	CDM has not developed policy/procedures for reviewing proposed configuration-controlled changes to the information system and approve/disapprove such changes with explicit consideration for security impact analyses.	Delayed	9/30/2017
	CDM does not define security configuration checklists to be used for CDM components to establish and document mandatory configuration settings for the information system technology products employed.	Delayed	9/30/2017
	CDM components are not configured to provide only essential capabilities.	Delayed	9/30/2017
	An inventory of CDM and subcomponents has not been developed or documented that accurately reflects the current information system, includes all components within the authorization boundary of the information system and is at the level of granularity deemed necessary for tracking and reporting.	Delayed	9/30/2017
	A configuration management plan has not been developed, documented or implemented that addresses, roles, responsibilities or configuration management processes and procedures.	Delayed	9/30/2017
	CDM does not perform vulnerability scanning of the information system and hosted applications monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported.	Delayed	9/30/2017
	CDM components do not identify, report, or correct system flaws.	Delayed	9/30/2017
Mike Monroney Aeronautical Center Trusted Internet Connection	The assessment team determined that an automated change management tool/mechanism is not in place.	Delayed	10/1/2017
	The assessment team determined that configuration settings are not configured in accordance with DOT required security configuration checklists.	Delayed	12/30/2017
	The assessment team determined that configuration settings, ports, protocols and services are not configured in accordance with DOT required security configuration checklists.	Delayed	12/30/2017

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	The assessment team determined that automated mechanisms are not employed with a maximum five minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system.	Delayed	12/30/2017
	The assessment team determined recently identified vulnerabilities have not been remediated within required time frames.	Delayed	9/30/2017
AIT Databases	Vulnerability scans are not performed on a monthly basis.	Delayed	3/31/2018
Enterprise Architecture and Solutions Environment	Telnet services cannot be disabled for EASE, which is recommended by FAA's vulnerability scanning software. At the time of our review, this POA&M was in a Delayed Status with a planned finish date of 5/5/2018. The FAA reported this POA&M was closed following our review.	Closed-Post Review	Not available
	Monthly credential vulnerability scans for EASE components are not implemented. At the time of our review, this POA&M was in a delayed status with a planned finish date of 5/5/2018. FAA reported this POA&M was closed following our review.	Closed-Post Review	Not available
Designee Management System	WebInspect and DB Protect scans are not being conducted on the DMS assets as required in the DOT compendium.	Delayed	9/30/2017
	WebInspect and HP Fortify scan results were not provided at the time of this assessment to determine whether the web applications or source code contain any security vulnerabilities.	Delayed	9/30/2017
NACIP (National Automated Conformity Inspection Process)	Evidence was not provided to show that previous versions of the NACIP baseline configurations of are retained to support rollback.	Delayed	5/31/2018
	The assessment team could not determine that the system owner monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	Delayed	5/31/2018
	The system owner did not provide information describing (1) whether or not the NACIP system is reviewed to identify unnecessary and/or nonsecure functions, ports, protocols, and services, (2) how often the review is conducted, and (3) who conducts the review, and (4) whether or not unnecessary ports are disabled if/when they are found during the review.	Delayed	5/31/2018
	The system inventory list provided by the system owner did not match the inventory list generated from MKS.	Delayed	5/31/2018
	The system owner did not provide the NACIP Configuration Management Plan.	Delayed	5/31/2018
	The vulnerability scan run on 03/12/2017, identified 88 high and 72 medium vulnerabilities containing the same vulnerabilities identified in the 04/12/2017 scan. At the time of our review, this POA&M was in a Delayed Status with a planned finish date of 9/30/2017. FAA reported this POA&M is now cancelled as part of their POA&M management process.	Cancelled-Post Review	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	Since a similar set of vulnerabilities were identified in both the FY16 and FY17 Webinspect scan results, with an increased number of critical vulnerabilities in FY17, the assessment team determined that remediation is not occurring within required DOT timeframes. At the time of our review, this POA&M was in a Delayed Status with a planned finish date of 9/30/2017. FAA reported this POA&M is now cancelled as part of its POA&M management process.	Cancelled-Post Review	Not available
FAA Directory Services	Not all application are tested outside the production environment when changes are implemented. At the time of our review, this POA&M was in a Delayed Status with a planned finish date of 9/30/2017. FAA reported this POA&M was closed following our review.	Closed-Post Review	Not available
	The organization does not implement configuration settings based on the list of DOT OCIO approved security settings and CIS / DISA standards.	Delayed	9/30/2018
	The organization does not implement ports, protocols and services based on the list of DOT OCIO approved security settings and CIS / DISA standards.	Delayed	9/30/2018
	Atypical usage monitoring for Enterprise/Domain accounts is not in place for FAA Directory Services.	Delayed	9/30/2018
	Monthly MVM scans are not being run on all servers.	Delayed	9/30/2017
	The WebInspect scan on Microsoft Certificate Authority (CA) performed in October 2016 revealed 1 critical, 2 high, 2 medium and 14 low vulnerabilities.	Delayed	9/30/2017
Direct User Access Terminal II CSC	The Configuration Management processes and procedures have not been documented in accordance with ATO Security. Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan.	POA&M Not Found in CSAM	Not available
	The organization does not implement configuration settings based on the list of DOT OCIO approved security settings and CIS / DISA standards. Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan	POA&M Not Found in CSAM	Not available
	DUATS II CSC assets have open, potentially unneeded ports enabled (See full results to determine what ports are needed to be active for functionality). Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan	POA&M Not Found in CSAM	Not available
	DUATSS Configuration Management Plan, Document Number DUATSS-CMP-002 Rev 8, dated June 28, 2006, is not available for review. Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan	POA&M Not Found in CSAM	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	The assessors found open POA&Ms pertaining to vulnerability scanning that have passed their Planned/Scheduled Completion dates and have not been remediated and their status has not been updated. Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan	POA&M Not Found in CSAM	Not available
	According to the SSP, security-relevant software updates aren't implemented. Following our review, the FAA reported this system is being decommissioned. However, that does not negate the Department's requirement to input POA&Ms for weaknesses identified during this system's lifespan	POA&M Not Found in CSAM	Not available
WMSCR (Weather Messaging Switching Center Replacement Sustainment)	Baseline testing revealed a number of systems which do not meet the CIS required baseline requirements. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found in CSAM	Not available
	Webinspect scan have not been run on the WMSCR applications run on VMs on the IESP. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found in CSAM	Not available
	The SSP does not document how often security-relevant software is updated, how software/firmware notifications and updates are tracked, and how flaw remediation is performed on the system. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found in CSAM	Not available
ASDE-X (Airport Surface Detection Equipment - Model X)	The SCD does not represent the current configuration. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found in CSAM	Not available
	Based on the SSP, system assets are not configured in accordance with the applicable Secure Configuration Baseline Standards. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	ASDE-X components are not configured to provide only the necessary ports, protocols, and services. Nessus scans identified 87 critical, 389 high, and 807 medium vulnerabilities. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	The SCD does not reflect an accurate baseline of all ASDE-X components. Test results from the previous assessment identified software in use that has not been defined in the SCD. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	Based on the SSP, system flaws identified and reported by Vendors, US Cert, NCO, CSMC, and IRAT are not corrected. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
WHDE (Wind Hazard Detection Equipment)	Based on interview results, changes have not been made in a long time. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	Based on interview results, no real hardening was done on system components. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	The SSP does not specifically address the ports, protocols, services and physical devices required to be active on each WHDE asset to support system operation. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	Based on examination of existing POA&MS, WHDE has not updated the status or remediated a number of open POA&Ms that are past due for their Planned and/or Scheduled Completion dates. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
SWIM Terminal Data Distribution System	The STDDS system components (RedHat Linux) are not fully configured and hardened to CIS requirements. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	There is no evidence that the system is configured to provide only the required ports, protocols, and/or services as defined in the SSP. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	Based on test results, Red Hat servers are missing many patches. Nessus testing discovered 86 critical, 203 High and 352 Medium vulnerabilities, many related to missing security patches. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
Information Technology Asset Management System	An updated HWSW list was provided but the list was incomplete.	Delayed	9/29/2017
	The McAfee Vulnerability Manager (MVM) scan report (dated May 3, 2016) did not include all three (3) IP/components of the Information Technology Asset Management System (ITAMS) authorization boundary.	POA&M Not Found	Not available
	No WebInspect scans were provided for ITAMS during the FY17 assessment.	Delayed	9/28/2018
Hazard Identification, Risk Management & Tracking	The DbProtect scan conducted on March 1, 2016 identified three (3) high vulnerabilities related to improper access controls and misconfigurations.	Delayed	12/30/2017
ADAS (Automated Weather Observation System Data Acquisition System)	No specific checklists are used to set configuration settings of system operating systems and applications.	Delayed	9/30/2017
	Based on the SSP, the system is not configured to provide only the required ports, protocols, and/or services. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	The SSP does not sufficiently address if System Owners update the inventory of system assets as part of system installations, removals, and updates. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
	The SSP does not sufficiently address how the configuration management plan and procedures documents are protected and marked. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
	Web Application scans could not be performed, per the most recent assessment. There are open POA&Ms that passed their Scheduled Completion dates that have not been remediated and their status has not been updated. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
	Windows 2003 Server devices are no longer supported and need to be updated. The assessors noted that security-relevant software updates are not implemented. The SSP does not explicitly document how flaw remediation is performed. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
Parsons Data System	The assessors noted several open POA&Ms pertaining in the Risk Assessment control family that have passed their Planned and/or Scheduled Completion dates and their status has not been updated. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
CPDS (Critical Power Distribution System)	The SSP does not document the (1) types of changes to the system that are exempt from configuration control and (2) entity authorized to approve configuration-controlled changes to systems under their purview. . At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	The SSP does not identify and document exceptions from the mandatory checklist configuration settings for individual hardware/software assets. . At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	An artifact has not been provided as part of the FY14 ISCM assessment to validate that least privilege controls for configuration settings have been implemented. . At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	The assessors noted several open POA&Ms pertaining in the Risk Assessment control family that have passed their Planned and/or Scheduled Completion dates and their status has not been updated. . At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available
	The CPDS system is using non-supported assets including Windows Server 2003 and Windows XP, for which patches are no longer available. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M	POA&M Not Found	Not available

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
Airports Geographic Information System	The mitigation of known vulnerabilities is not occurring within required timeframes. At the time of our review, the first POA&M was in a Delayed Status with a planned finish date of 9/30/2017. The FAA reported this POA&M was closed following our review.	Closed-Post Review	Not available
		Delayed	12/31/2017
FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System	Based on results for Web Inspect scan testing, a number of system flaws have been identified requiring mitigation. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
Instrument Flight Procedures Automation-Mission Support	Testing of Windows assets shows high vulnerabilities associated with undocumented applications. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
	Analysis of recent DBProtect test results (August 2017) provided by ESC indicates that the IFPA Oracle database is significantly behind on patches and meeting compliance requirements. At the time of our review, a POA&M was not found in CSAM. Following our review, the FAA reported they created a POA&M.	POA&M Not Found	Not available
Real Property Financial Management Tool (RPFMT)	The assessors found high vulnerabilities that have not been remediated during this assessment.	In Progress	9/30/2018
Building Automation System	Based on examination of existing POA&Ms, CCMS has not updated the status or remediated a number of open POA&Ms that are past due for their Planned and/or Scheduled Completion dates.	Delayed	10/30/2016
	Some CCMS locations reported that no testing is performed prior to system updates.	Delayed	10/31/2016

FMCSA

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
FMCSA Service Centers	Based on the baseline scans for FMCSA workstations, servers and Cisco IOS network devices,	Delayed	12/30/2014
	FMCSA Service Centers' servers, workstations, and Cisco routers and switches have some ports, protocols and services that have not been prohibited or restricted.	Delayed	12/30/2014
	No particular test plan is used for software updates and the remediation of vulnerabilities on FMCSA information systems before installation.	In Progress	12/30/2015
SAFETYNET	The system does not have a fully developed and documented secure baseline configuration to validate the configuration settings.	POA&M Not Found	Not available
	The FMCSA Cloud Environment has not completed documenting procedures to identify system flaws.	POA&M Not Found	Not available

FRA

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
FRA HOSTS	The remote host supports the use of RC4 in one or more cipher suites. At the time of our review, this POA&M was in a Delayed status with a planned finish date of 9/20/2017. Following our review, the FRA reported they closed the POA&M on 9/8/2018.	Closed-Post Review	Not available
	It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.	Delayed	9/20/2017

FTA

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
FTA General Support System (GSS)	Deviations from the latest/recent CIS Benchmarks scans (Conducted during the month of August 2017) are not documented or approved.	Delayed	3/6/2018
	The FTA GSS Configuration Management Plan does not exist.	In Progress	6/6/2018
	Scans conducted on 8/29/2017 showed 3 high findings for administrator users' passwords never expiring.	Delayed	12/27/2017
	System flaws are reported in a number of ways that include weekly MVM scanning, database scanning, annual web inspect scanning, and CIS compliance scanning. Multiple scans show vulnerabilities and evidence of remediation was not provided.	Delayed	12/27/2017

MARAD

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
MARAD Internet	A current baseline configuration of the information system has not been developed.	Delayed	TBD
	The types of changes to the information system that must be configuration-controlled are not documented.	Delayed	TBD
	Security configuration checklists to be used to establish and document configuration settings for the information technology products employed by the system have not been defined.	Delayed	TBD
	The system is not configured to provide only essential capabilities.	Delayed	TBD
	An inventory of information system components that accurately reflects the current information system has not been developed or documented.	Delayed	TBD
	A configuration management plan has not been provided.	Delayed	TBD
	MARAD Internet does not employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned	Delayed	TBD

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
	MARAD Internet does not (1) use a test environment to test patch effectiveness prior to installing patches and (2) implement automated mechanisms for flaw remediation updates.	Delayed	TBD
Comprehensive Academic Management System (CAMS)	Unspecified weaknesses associated with Configuration Management were identified during the FY 2015 assessment.	Delayed	TBD

OIG

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
JA-20 Lab	The JAB does not define information system components or operational requirements for which any deviations from established configuration settings are identified, documented, and approved.	Delayed	5/1/2017 6/28/2018

OST

System Name	Weakness Description (OIG Summary)	Status	Planned Finish Date
Volpe Physical Access Control System	The VPACS application server (DH6PV94) uses an unsupported build version of Microsoft SQL Server 2008 R2.	Not Started	TBD

Source: OIG analysis.

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

FAA: High and Moderate Impact Systems

System Name	Description of Weakness	Status	Planned Finish Date
FAA Continuous Diagnostics and Mitigation	The RES application does not select user account groups that are critical to the system's business function and does not document them within the CDM System Security Plan.	Delayed	9/30/2017
	CDM has not defined duties of the system users for all CDM subcomponents and has not documented those defined duties of system users in the CDM System Security Plan	POAM Not Found in CSAM	Not available
	CDM does not define security functions deployed in the hardware within the system security plan.	Delayed	9/30/2017
	BigFix, ForeScout, and RES do not display a system use notification that complies with DOT Compendium policy prior to granting access to the system.	Delayed	9/30/2017
	BigFix is not using multifactor authentication for local access to privileged accounts in the R&D environment for users and in the Mission Support environment for the BES Admin shared account.	Delayed	9/30/2017
	CDM does not have a mechanism in place to enforce changing/refreshing information system authenticators every 60 days.	Delayed	9/30/2017
Mike Monroney Aeronautical Center Trusted Internet Connection	ForeScout, Bluecoat and Checkpoint Firewall components are not automatically disabled after 90 days of inactivity.	Delayed	9/30/2017
	The MMAC TIC does not implement multifactor authentication for network access or administrator access.	Delayed	9/30/2017
	Authenticators do not meet strength and lifetime requirements and are not refreshed every 60 days.	Delayed	12/30/2017
AIT Databases	The monthly database scan tool, Database Protect (DbProtect), identifies the Remote login password file, which is enabled, as a high risk vulnerability.	Delayed	8/31/2018
	Authentication to Windows servers and MS SQL databases is performed through usernames and passwords via Integrated Windows Authentication (IWA) or local credentials.	Delayed	8/31/2018
Designee Management System	Although DMS user accounts, privileged and non-privileged, are reviewed on a regular basis, these reviews are not documented.	Delayed	9/30/2017
	DMS is currently not auditing the execution of privileged functions.	Delayed	9/30/2017
	The DMS internal component does not display the required System Use Notification banner prior to allowing access to the system.	Delayed	9/30/2017
	Although the registered users' (applicants, designees) passwords for the DMS external application meet the requirements of password complexity as outlined in FAA policy, the password does not comply with the DOT's requirement of 12 characters in length or that no character may be repeated twice in sequence.	Delayed	9/30/2017

System Name	Description of Weakness	Status	Planned Finish Date
NACIP (National Automated Conformity Inspection Process)	Evidence was not provided to indicate that defined personnel or roles are being notified upon user account creation, modification, enabling, disabling, and removal actions.	Delayed	5/31/2018
	The system owner did not provide documentation describing and/or describe how external user passwords are managed for the NACIP system and whether or not authenticators are required to be changed/refreshed every 60 days.	Delayed	5/31/2018
FAA Directory Services	A process does not exist where accounts are reviewed semi-annually for privileged accounts and annually for non-privileged accounts.	Delayed	9/30/2017
	The webpages for the tools within the boundary do not have the required DOT warning banner.	Delayed	9/30/2017
	Multifactor authentication for privileged accounts for network access to the domain controllers and servers within scope is not implemented.	Delayed	9/30/2017
	The information system does not implement the required authenticator requirements on all assets.	Delayed	3/10/2017
Direct User Access Terminal II CSC	There is an annual account review for HP-UX/TRU64, Redhat, and the DUAT application accounts by CSC DUAT system administrators.	POAM Not Found in CSAM	Not available
	Not all system components contain a valid FAA warning banner in accordance with FAA Order 1370.102.	POAM Not Found in CSAM	Not available
	DUATS assets are not capable of using PIV credentials in accordance with FIPS 201.	POAM Not Found in CSAM	Not available
	The assessors found not all system components enforce authenticator strength in accordance with the applicable Secure Configuration Baseline Standards.	POAM Not Found in CSAM	Not available
WMSCR (Weather Messaging Switching Center Replacement Sustainment)	The SSP fails to identify and document all operating system account types for all system assets.	POAM Not Found in CSAM	Not available
	Based on the examination of the SSP and interview results, administrators have the same level of access and there is no separation of duties.	POAM Not Found in CSAM	Not available
	The assessors found no evidence to validate that WMSCR has been configured so that all system accounts (OS, iOS) with shared identifiers require logging in to a unique account prior to accessing the system's shared administrator accounts.	POAM Not Found in CSAM	Not available
	Based on the examination of the SSP, it does not document the authorized privileged functions (e.g., configuring access privileged setting events to be audited, setting intrusion detection parameters) that can be accessed remotely and the rationale for providing remote access to the privileged functions.	POAM Not Found in CSAM	Not available
	The assessors found no Identity and Access Management procedures documented in accordance with the ATO ISS Procedures Guidance.	POAM Not Found in CSAM	Not available
ASDE-X (Airport Surface Detection Equipment - Model X)	The SSP does not address the procedures and responsibilities for requesting and approving account creation.	In Progress	9/30/2018
	The ASDE-X SSP does not document how the system prevents non-privileged users from executing privileged functions including disabling, circumventing, or altering implemented security safeguards/ countermeasures.	POA&M Not Found in CSAM	Not available

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

System Name	Description of Weakness	Status	Planned Finish Date
	Based on test results, not all components have FAA-approved warning banners. Per the review of the SSP, compensating controls and controls for handling assets that require account lockout are not documented.	Delayed	9/30/2018
	According to the Security Characterization Document, not all assets have unique accounts configured.	Delayed	9/30/2017
	Based on the examination of the SSP dated December 2015, OS level passwords are not changed from default.	Delayed	12/31/2018
WHDE (Wind Hazard Detection Equipment)	There is no capability to generate an authorized user list for shared accounts used on ASTI.	POAM Not Found in CSAM	Not available
	All ASTI administrators have the same privileges.	POAM Not Found in CSAM	Not available
	Not all web applications display a warning banner.	POAM Not Found in CSAM	Not available
	For the shared ASTI accounts the SSP does not (1) document every access method/point by type (e.g., local access to Applications, OSs, and assets) that does not require a unique identifier/authenticator, (2) what specific privileges are provided via the access method/point, and (3) compensating controls.	POAM Not Found in CSAM	Not available
	ASTI Authenticator Management procedures have not been fully developed and documented as defined in the ATO ISS Procedures Guidance.	POAM Not Found in CSAM	Not available
ARSR 1/2 (Air Route Surveillance Radar Models 1 & 2)	Formal access control procedures conforming to the ATO ISS Procedures Guidance have not been developed.	Delayed	4/16/2012
	The SSP does not document (1) every access method/point by type (e.g., local access to Applications, OS's, and assets) that does not require a unique identifier/authenticator, (2) what specific privileges are provided via the access method/point, and (3) compensating controls.	Delayed	4/16/2012
	FAA approved complexity is not enforced on the system's RPP passwords.	Delayed	4/16/2012
SWIM Terminal Data Distribution System	The RedHat application server was not designated as an ICS asset.	POAM Not Found in CSAM	Not available
	The SSP indicates that the MCD application expires passwords after 90 days and switches are configured with 13 character passwords, which are not changed. This was not confirmed by the data collected during testing.	POAM Not Found in CSAM	Not available
IVSR (Interim Voice Switch Replacement System)	The IVSR currently uses the inherent capabilities of Microsoft Server 2003 software for account management.	POAM Not Found in CSAM	Not available
	The System Owner will discuss this with Second Level Engineering Support to develop a policy and the associated implementation plan (pertaining to access control).	POAM Not Found in CSAM	Not available
	Authenticators are not changed/refreshed in accordance with FAA policy.	POAM Not Found in CSAM	Not available

FAA: Low Impact Systems

System Name	Description of Weakness	Status	Planned Finish Date
Information Technology Asset Management System	ITAMS does not document key access control procedures or enforce access control mechanism for its application for users based on limited access/need to know principles.	Delayed	8/31/2018
ADAS (Automated Weather Observation System Data Acquisition System)	Based on the examination of the SSP, The SSP does not document personnel that are responsible for account management.	Delayed	9/30/2018
	Based on the examination of the SSP dated May 2016, user account privileges are not implemented to provide separation of duties.	Delayed	9/30/2018
	Based on the examination of the SSP dated May 2016, it fails to document how the account privileges explicitly authorize access to security functions and how the user accounts enforce using non-privileged accounts, and only allow privileged account usage for Security Related and System Administrative functions.	Delayed	9/30/2018
	ADAS Windows and Redhat devices did not display a warning banner in accordance with FAA Order 1370.102, as part of every system login prior to system access.	Delayed	9/30/2018
	Based on the SSP, there are currently no Authenticator Management procedures developed. .	Delayed	9/30/2018
	Based on the examination of the SSP, authenticator strength is not configured in accordance with the applicable Secure Configuration Baseline Standards.	Delayed	9/30/2018
CPDS (Critical Power Distribution System)	Based on the SSP, the Cisco VPN Network Appliance is not documented.	POAM Not Found in CSAM	Not available
	The SSP states that CPDS does not enforce the concept of least privilege at the OS or at the application level.	POAM Not Found in CSAM	Not available
	From the previous assessment: None of the system components are configured with a warning banner.	POAM Not Found in CSAM	Not available
	From the previous assessment: A device has auto login turned on and that anyone can log into the device over the network with a default (known) username and password pair.	POAM Not Found in CSAM	Not available
	From the previous assessment: Based on the results of the interviews passwords for system components are never changed.	POAM Not Found in CSAM	Not available
Airports Geographic Information System	AGIS does not have a formal process explicitly addressing user account management provisioning (approving, adding, updating, removing, etc.) and annual review/recertification of user accounts.	Delayed	5/31/2018
	A system use notification message and warning banner is presented to all users of the AGIS system, however, the system does not "retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system."	Delayed	5/31/2018

System Name	Description of Weakness	Status	Planned Finish Date
FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System	The SSP fails to address if emergency or temporary user accounts are used and if disabling is done within 24 hours after the need for the account is no longer valid.	POAM Not Found in CSAM	Not available
	Based on the latest SSP, FEATS does not enforce the latest password policies which requires the use of one upper, one lower, one number, and one special character.	POAM Not Found in CSAM	Not available
Instrument Flight Procedures Automation-Mission Support	The SSP fails to describe what mechanism are used to maintain a list of users for each account type for the system.	POAM Not Found in CSAM	Not available
Building Automation System	CCMS generally utilizes one shared account for access.	Delayed	10/31/2016
	The SSP does not document the concept of least privilege when establishing system user accounts.	Delayed	10/31/2016
	An approved FAA security warning banner is not displayed prior to accessing CCMS.	Delayed	10/31/2016
	The SSP does not describe system logical access methods/points use unique identifiers and authenticators	Delayed	10/31/2016
	CCMS passwords/authenticators are not complex and do not meet DOT standards.	Delayed	10/31/2016

FMCSA

System Name	Description of Weakness	Status	Planned Finish Date
FMCSA Service Centers	Formal notification is not usually sent when information system usage or need-to-know/need-to-share changes.	Delayed	12/30/2014
		In Progress	12/30/2015
	FMCSA does not fully separate the duties of individuals as necessary, to prevent malevolent activities without collusion.	Delayed	12/30/2014
	The required minimum permission levels for test installations of desktop applications are not always provided to FMCSA Technical Infrastructure Team to ensure that the correct permission levels are applied and hashes generated to allow users to run the updated authorized version.	Delayed	12/30/2014
	The login banner associated with McAfee Endpoint Encryption for laptops did not use an approved banner.	In Progress	12/30/2015
	The local admin accounts are shared for both servers and workstations.	In Progress	12/30/2015
FMCSA does not define the time period (by authenticator type) for changing/refreshing authenticators.	In Progress	12/30/2015	

System Name	Description of Weakness	Status	Planned Finish Date
SAFETYNET	Inconsistencies were identified pertaining to who is required to approve FMCSA accounts.	POAM Not Found in CSAM	Not available
	Need evidence to support multifactor authentication for network access to privileged accounts.	POAM Not Found in CSAM	Not available
	Need evidence to support FMCSA manages information system authenticators by changing default content of authenticators prior to information system installation	POAM Not Found in CSAM	Not available

FRA

System Name	Description of Weakness	Status	Planned Finish Date
FRA HOSTS	The DMZ Linux proxy server uses its own datastore and does not have an automated method to manage accounts.	Delayed	9/20/2017
	Linux servers do not force passwords to be changed, do not enforce password minimum and maximum lifetime restrictions, and do not prohibit password reuse.	Delayed	9/20/2017

FTA

System Name	Description of Weakness	Status	Planned Finish Date
FTA General Support System (GSS)	A formal documented process has not been created for other applications to specify authorized users, role/group membership, and access authorizations for new accounts.	Delayed	3/6/2018
		Delayed	3/6/2018
		In progress	6/6/2018
	No documentation was provided to show what personnel or roles have privileged accounts on applications.	Delayed	3/6/2018
	Not all applications display a DOT-approved warning banner.	POAM Not Found in CSAM	Not available
	Not all applications use multi-factor authentication.	In Progress	6/6/2018

MARAD

System Name	Description of Weakness	Status	Planned Finish Date
MARAD Internet	This control is inherited from the MARAD COE, which has an open Account Management POA&M (58609).	Pending	9/29/2017
	The MARAD Internet FY11 SA ISSP neither defines or documents any how automated mechanisms enforce the implementation of separation of duties.	POAM Not Found in CSAM	Not available
Comprehensive Academic Management System (CAMS)	Existing POA&M: Unspecified access control findings from the FY 15 assessment are currently open with no planned finish date.	Delayed	TBD
	Existing POA&M: Unspecified identification and authentication findings from the FY 15 assessment are currently open with no planned finish date.	Delayed	TBD

OST

System Name	Description of Weakness	Status	Planned Finish Date
Volpe Physical Access Control System	Domain user accounts exist for individuals who no longer require access. At the time of our review, this POA&M had not been started with a planned finish date of "TBD". Following our review, Volpe reported they closed the POA&M on 7/10/2018.	Closed-Post Review	Not available
	The SQL Server default SA account on the V-PACS SQL database server is not disabled.	Not Started	TBD
Volpe MSEPM (Microsoft Enterprise Project Management)	Separation of duties is not clearly defined for system support functions. At the time of our review, this POA&M had not been started with a planned finish date of "TBD". Following our review, Volpe reported they closed the POA&M on 6/20/2018	Closed-Post Review	TBD
	A shared folder on the database server is not properly restricted.	Not Started	TBD
Common Operating Environment (COE)	The Assessment Team found VDI provides the option for multi-factor authentication, but is not enforced.	Not Started	9/30/2019

Source: OIG analysis.

Exhibit G. System Weaknesses in Data Protection and Privacy, by OA

FAA

System Name	Weakness Description	Status	Planned Finish Date
Mike Monroney Aeronautical Center Trusted Internet Connection	The information system does not employ integrity verification tools to detect unauthorized changes on all system components.	Delayed	12/30/2017
AIT Databases	Transparent Data Encryption (TDE) to protect the AIT Databases data is not turned on for all databases.	Delayed	9/29/2017
Enterprise Architecture and Solutions Environment	Privacy controls are inherited from DOT SOC, FAA Domain, MMAC NET, MMAC TIC, and NITC Datacenter.	Not available	Not available
NACIP (National Automated Conformity Inspection Process)	The PTA and PIA have not been updated. At the time of our review, an updated PTA was not yet completed. Following our review, the FAA provided an updated PTA.	Delayed	5/31/2018
	The internal NACIP URL does not provide SSL encryption.	Delayed	5/31/2018
Federal Aviation Administration Directory Services	The system does not have an adjudicated PTA from the DOT Privacy Office to determine whether a Privacy Impact Assessment is required. Without an adjudicated PTA, the system owner does not know whether a PIA will be required and may cause legal issues if it is operational using PII but does not have a published PIA.	Delayed	9/30/2018
Direct User Access Terminal II CSC	Based on the SCD, the PTA has expired, and the new PTA was submitted on January 22, 2016. It's currently with the Records Schedule POC for review and approval. At the time of our review, an updated PTA was not yet completed. Following our review, the FAA provided an updated PTA.	Delayed	9/30/2017
	Media Protection procedures for CSC DUATS are not available for review. It is uncertain at which level this is really implemented.	Not available	Not available
	DUATS stores pilot information that may contain Social Security Numbers in a MySQL Database that does not implement encryption.	Delayed	12/1/2016
	The Unix Web servers do not have anti-virus software installed. Scans are not performed at least weekly. Real-time scans of files from external sources as the files are downloaded, opened, or executed are not performed. The servers are not configured to block malicious code and/or quarantine malicious code in response to malicious code	All Delayed	5/31/2017 4/28/2017 12/1/2016 4/28/2017 4/28/2017

System Name	Weakness Description	Status	Planned Finish Date
	detection. Malicious code protection mechanisms updates are not automated.		10/1/2012 5/31/2017
	No procedures have been developed by CSC DUATS to alert the NCO/CSMC when Security Incidents are detected.	Delayed	12/1/2016
IVSR (Interim Voice Switch Replacement System)	Media Protection procedures for media sanitization and disposal are not documented. In addition, compensating controls are not identified.	Delayed	9/30/2017
Hazard Identification, Risk Management & Tracking	See findings for common control providers AIT EDC, WHJTC, FAA SOC, MMAC TIC	Not available	Not available
Airports Geographic Information System	The Assessment Team found AGIS employs a weak SSL protocol: TLS 1.0. Assessor confirmed control is not implemented and reviewed status of existing findings and progress towards remediation of POA&M #58761. The assessor noted there has been no progress on the POA&M due to staff turn-over.	Delayed	5/31/2018

FHWA

System Name	Weakness Description	Status	Planned Finish Date
User Profile and Access Control System	The most recent PIA was completed in August 2004. An updated PIA was submitted to OST on 4/12/18 for adjudication. Following our review, the FHWA provided an updated PIA.	Not available	Not available
Freedom Of Information Act System	PIA is outdated. An updated PIA was submitted to OST on 3/14/18 for adjudication.	Not available	Not available

FMCSA

System Name	Weakness Description	Status	Planned Finish Date
FMCSA Service Centers	The Privacy Impact Assessment (PIA) is out of date. The most recent PIA is dated June 15, 2008. This system has not been assessed since 2012. According to system authorization documentation, this system collects the following data points: Name Date of Birth, Home Address, Driver's License Number, Phone Number, Mother's Maiden Name, Social Security Number, and Medical Information.	POAM Not Found in CSAM	Not available
SAFETYNET	The Privacy Impact Assessment (PIA) is out of date and should be updated to reflect the current status of the system. This system has not been assessed since 2016. The PIA was submitted to the department's Chief Privacy Office on 11/2/2016. Currently, the PIA is still pending DOT Chief Privacy Office approval. According to system authorization documentation, this system collects the following data points: Name Date of Birth, Home Address, Driver's License Number, Phone Number, and Social Security Number.	POAM Not Found in CSAM	Not available

FRA

System	Weakness Description	Status	Planned Finish Date
FRA Hosting and Operational Support Technology Service (HOSTS)	Digital PII is not redacted or de-identified on the FRA-HOSTS network.	Delayed	9/20/2017
	According to system documentation, HOSTS contains PII and FRA has not finalized the system's Privacy Impact Assessment (PIA). According to security authorization documentation, this system collects the following data points: Name, Home Address, Date of Birth, Place of Birth, Medical Information, Social Security Number, Race Age, Marital Status, and Financial Information.	POAM Not Found in CSAM	Not available
Railroad Enforcement System	The current Privacy Impact Assessment (PIA) and Privacy Threshold Analysis (PTA) documentation for the system are out of date. According to the most recent PIA we reviewed (January 31, 2012), this system collects the following data points: Name, Date of Birth, Address, Phone Number, and Email Address.	Delayed	5/27/2016

FTA

System	Weakness Description	Status	Planned Finish Date
FTA General Support System (GSS)	Server logs are sent to the FTA SIEM tool, however, the assessors were unclear which events the SIEM tool is configured to monitor for and alert. The FTA has not defined monitoring objectives and indicators of compromise or potential compromise. The assessors were unclear how the FTA identifies unauthorized use of information systems. Database level logs are not sent to the SIEM tool for monitoring and the assessors were unclear if Windows IIS logs are sent to the SIEM tool.	Delayed	3/6/2018
	No integrity verification tools are used to detect unauthorized changes to the servers.	Delayed	3/6/2018

MARAD

System	Weakness Description	Status	Planned Finish Date
Comprehensive Academic Management System (CAMS)	The DOT CPO has determined that the CAMS collects personally identifiable information on individuals and constitutes a privacy sensitive system. Thus a Privacy Impact Assessment (PIA) is required. Information in this system is retrieved by a personal identifier and meets the standard for a system of records as defined by the Privacy Act. The appropriate systems of records notices for records related to the primacy purpose of the system as MARAD-12, 16, 27, 29. Given the consolidation of the systems identified in these SORNs, MARAD should review these notices and publish, update, retire the notices as appropriate.	Pending	9/28/2018

NHTSA

System	Weakness Description	Status	Planned Finish Date
NHTSA119: Grants Management Solutions Suite	Security and privacy controls are inherited from the DOT/FAA SOC. See control deficiencies outlined in the common control provider section.	Not available	Not available
NHTSA009: Fatality Analysis Reporting Sys.	We found the Privacy Impact Assessment (PIA) has not been reviewed or updated since 2003. In addition, OIG did not find evidence of a current Privacy Threshold Analysis (PTA). According to system documentation, this system collects the following data points from individuals involved in motor vehicle incidents and organizations requesting crash data: Name, Home Address, Date of Birth, Age, Gender, Driver's License Number and Status, Blood Alcohol Content, Death Certificate Number, and Race. This system has not been assessed for security weaknesses since 2015.	A POA&M was not found in CSAM	Not available

OST

System	Weakness Description	Status	Planned Finish Date
Volpe Physical Access Control System	OIG does not have evidence of a finalized PTA.	POAM Not Found in CSAM	Not available
	Not all V-PACS servers have software installed to detect changes to system configuration. The backup server is the only V-PACS server that is deployed with a File Integrity Manager agent.	Not Started	TBD
Volpe MSEPM (Microsoft Enterprise Project Management)	This system inherits security and privacy controls from the Volpe LAN. See deficiencies identified for the common control provider-OST COE.	Not available	Not available
Common Operating Environment (COE)	Software integrity checking software/tools are not implemented. There are no tools that perform automated notification of software integrity verification failures. Also, there are no notification procedures to educate personnel on the notification process for when integrity verification fails. The COE does not respond automatically when integrity violations are discovered. There are no tools to assist with detecting changes to the COE. Also, these changes (once discovered) would not be incorporated into the organizational incident response capability.	Not Started	3/30/2019

System	Weakness Description	Status	Planned Finish Date
Parking and Transit Benefit System	This system inherits security and privacy controls from the DOT COE. See deficiencies identified for the common control provider-OST COE.	Not available	Not available

PHMSA

System	Weakness Description	Status	Planned Finish Date
Hazardous Materials Information System	This system inherits security and privacy controls from the DOT COE. See deficiencies identified for the common control provider-OST COE.	Not available	Not available

Source: OIG analysis

Exhibit H. Weaknesses in Incident Response in Sample Systems, by OA

FAA

System Name	Status	Weakness	Planned Finish Date
AIT Databases	Delayed	The system does not have a documented incident handling plan, process or capability. Moreover, the system has not had a security incident which would have triggered an incident response capability. Therefore, the assessment team could not verify the incident handling capability or processes of the system.	9/30/2017
Federal Aviation Administration Directory Services	Delayed	No tests and/or exercises have been conducted for an incident response capability to determine the incident response effectiveness. Formal incident response training is not provided for users with assigned roles.	9/30/2017
WMSCR (Weather Messaging Switching Center Replacement Sustainment)	In Progress	Based on the examination of the WMSCR SSP, there are no Incident Response procedures developed in accordance with ATO Procedural Guidance.	3/31/2018
	Unknown	Based on the examination of the SSP dated January 2015, there are some system level Incident Response procedures documented, however they have not been developed in accordance with ATO ISS Procedures Guidance. Based on the examination of the SSP dated January 2015, there is no WMSCR specific- incident reporting procedure.	Unknown
WHDE (Wind Hazard Detection Equipment)	In Progress	A number of system procedures have not been documented (or appropriately referenced) within the SSP under the appropriate control section, in accordance with ATO Security Requirements.	1/2/2016
	Unknown	Based on interview results, personnel were not sure who they would contact at this time. No procedures are documented.	Unknown
VRRP/DALR (Voice Recorder Replacement Program/Digital Audio Legal Recorder)	In Progress	There are no VRRP/DALR Incident Response procedures developed as defined in ATO ISS Procedures Guidance. There are no VRRP-DALR Incident Response procedures developed and implemented. Based on examination of the SSP dated February 2017 (FY17 VRRP/DALR SSP), there is no specific reference to any Incident Response procedures.	9/29/2017
IVSR (Interim Voice Switch Replacement System)	In Progress	A number of system procedures have not been documented (or appropriately referenced) within the SSP under the appropriate control section, in accordance with ATO Security Requirements.	3/30/2016
Information Technology Asset Management System	Pending	The System Owner did not provide evidence showing that Incident Response training was conducted in FY17.	8/31/2018
Real Property Financial Management Tool (RPFMT)	Pending	Incident response training has not been provided to users with assigned roles and responsibilities because RPFMT is still in development and users are not using RPFMT.	6/30/2018
Building Automation System	Delayed	Incident Response Procedures in accordance with ATO ISS Procedures Guidance have not been developed.	10/31/2016

FMCSA

System Name	Status	Weakness	Planned Finish Date
FMCSA Service Centers	Delayed	DOT Cybersecurity Compendium requires that DOT Components must provide its Component-specific incident handling procedures to the DOT CISO and DOT CSIRC.	12/30/2014
	Delayed	Although the FMCSA IT Systems SOP MC-05 for Computer Incident Handling and Reporting is posted on FMCSA Intranet website, KnowZone, the distribution list does not include Network Services Team or Field Technical Support (i.e. FMCSA Technical Infrastructure Team) which accounts to them not being knowledgeable of the FMCSA IR procedure.	12/30/2014
	Delayed	Neither the FMCSA Order 1641.1: Cyber Security Incident Handling and Reporting nor FMCSA IT Systems Standard Operating Procedure MC-05 for Computer Incident Handling and Reporting have been reviewed or updated since being posted which is more than three years. Some information is no longer current such as contacts.	12/30/2014
	In Progress	FMCSA has never conducted tests/exercises on the IR capability for FMCSA Service Centers' information systems using NIST SP 800-61 tests/exercises.	12/30/2015
	In Progress	Since no tests/exercises are conducted, FMCSA does not document the results of incident response tests/exercises.	12/30/2015
	In Progress	FMCSA does not have all the appropriate tools and resources to accomplish forensic work required in a timely manner.	12/30/2015
	In Progress	FMCSA does not coordinate incident handling activities with contingency planning activities.	12/30/2015
	Delayed	FMCSA does not employ automated mechanisms to increase the availability of incident response-related information and support.	12/30/2014
	In Progress	FMCSA does not have an incident response plan.	12/30/2015

Source: DOT

Exhibit I. OIG's Previous FISMA Reports

DOT's Information Security Posture Is Still Not Effective (OIG Report Number FI2018017), January 24, 2018

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 (OIG Report Number FI-2014-006), November 22, 2013

Ongoing Weaknesses 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 J. Open Recommendations from Previous FISMA Reports

Fiscal Year 2017, OIG Report Number FI-2018-017

Number	Recommendation
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. [OPEN and UNRESOLVED]
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. [OPEN and UNRESOLVED]
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.

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) POA&Ms 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 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
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.
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 planned completion dates to monitor and track progress. [still OPEN – missing from FISMA 2017 report]
16	Work with the Director of DOT Security to develop or revise their plans to effectively transition the remaining facilities to required PIV cards.

Fiscal Year 2013, OIG Report Number FI-2014-006

Number	Recommendation
1	Obtain and review specialized training statistics and verify, as part of the compliance review process, that all employees with significant security responsibilities have completed the number of training hours required by policy. Report results to management and obtain evidence of corrective actions.
4	Obtain and review plans from FMCSA, MARAD, OST, and RITA to authorize systems with expired accreditations. Perform security reviews of unauthorized systems to determine if the enterprise is exposed to unacceptable risk.
7	Obtain a schedule and action plan for OAs to develop procedures for comprehensive cloud computing agreements to include security controls roles and responsibilities. Report to OA management any delays in completing the procedures.
8	Obtain and review existing cloud computing agreements to assess compliance with agency policy, including security requirements. Report exceptions to OA management.

Fiscal Year 2011, OIG Report Number FI-2012-007

Number	Recommendation
1	Enhance existing policy to address security awareness training for non-computer users, address security costs as part of capital planning, correct the definition of "government system", and address the identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications.
3	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.

Fiscal Year 2010, OIG Report Number FI-2011-022

Number	Recommendation
14	Identify and implement automated tools to better track contractors and training requirements.

Source: OIG

Exhibit K. List of Acronyms

CIO	Chief Information Officer
CISO	Chief Information Security Officer
COE	common operating environment
CSMC	Cybersecurity Management Center
DOT	Department of Transportation
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FITARA	Federal Information Technology Acquisition and Reform Act of 2014
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IT	information technology
MARAD	Maritime Administration
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute 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 identity verification
POA&M	plan of action and milestones
US-CERT	United States Computer Emergency Readiness Team
Volpe	John A. Volpe National Transportation Systems Center

Exhibit L. Major Contributors to This Report

KEVIN DORSEY	PROGRAM DIRECTOR
STACY JORDAN	PROJECT MANAGER
TRACY COLLIGAN	SENIOR INFORMATION TECHNOLOGY SPECIALIST
JENELLE MORRIS	SENIOR INFORMATION TECHNOLOGY SPECIALIST
JO'SHENA JAMISON	SENIOR INFORMATION TECHNOLOGY SPECIALIST
ZACHARY SCOTT	AUDITOR
ALLISON LA VAY	SENIOR MANAGEMENT AND PROGRAM ANALYST
FRANCISCO RAMOS HILERIO	SENIOR AUDITOR
PETRA SWARTZLANDER	SENIOR STATISTICIAN
MAKESI ORMOND	STATISTICIAN
SUSAN NEILL	WRITER-EDITOR

Appendix. Agency Comments



**U.S. Department of
Transportation**

Office of the Secretary
of Transportation

Memorandum

Subject: **ACTION**: Management Response to the OIG Draft Report—
FISMA 2018: Project No. 18F3009F000

From: Kristen Baldwin
DOT Deputy Chief Information Officer

KRISTEN K. BALDWIN
Digitally signed by KRISTEN K.
BALDWIN
Date: 2019.03.01 13:43:07 -05'00'

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

At the beginning of fiscal year (FY) 2018, the Department held an overall rating from the Department of Homeland Security (DHS) of “At Risk”, under the framework and risk management assessment (RMA) methodology established by Executive Order (EO) 13800 on “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” By interweaving cybersecurity throughout the Department’s strategic plan and establishing it as a leadership priority, the Department improved on its performance, increasing to a DHS RMA rating of “Managing Risk” by the end of FY 2018. This was accomplished by focusing on:

- Increasing the number and percentage of systems authorized to 457 of 459 (99.6%) across DOT, and 34 of 35 (97%) with the Office of the Secretary (OST), and ensuring that high impact and moderate impact systems had authorizations to operate (ATOs);
- Replacing legacy mobile device management solutions with a single, enterprise solution from Microsoft to improve upon the agency’s ability to remotely secure more than 6,000 smartphones and tablets;
- Expanding upon the Department’s deployment of Continuous Diagnostics and Mitigation (CDM) capabilities for hardware and software asset management to improve enterprise coverage and visibility;
- Remediating critical vulnerabilities for public-facing web sites and systems in 30 days or less; and
- Ensuring that agency high-value asset systems had information security contingency plans, and alternate processing sites – notably at the Stennis data center and in DOT-approved cloud environments - for continued operations or recovery after an incident.

Under extraordinary leadership by the Chief Information Officer (CIO), and through the Department's Information Technology (IT) transformation initiative, DOT achieved additional, notable improvements in its cybersecurity posture during FY 2018 to include:

- Execution of an Interagency Agreement with the General Services Administration (GSA) for use and support of GSA's login.gov strong authentication services for the American public, and non-DOT stakeholders, and integration of those services into DOT public-facing websites and applications;
- Modernization of a significant system in the Federal Motor Carrier Safety Administration, which eliminated multiple vulnerabilities from legacy technology, and integrated the use of GSA's strong authentication services provided by Login.gov;
- Consolidation of multiple IT contracts into the DOT CIO's enterprise IT services contract to improve efficiencies, reduce costs, improve the consistency of services and controls, and to reduce cybersecurity risks resulting from disparate contracts and controls implementation;
- Advancement of the DOT Network Assessment Risk Mitigation (NARM) initiative into its next phase which includes cybersecurity monitoring, threat detection, and automated response capabilities;
- Development of processes and tools to automate and accelerate deployment of Microsoft Windows 10 Enterprise to computers managed within the Common Operating Environment (COE), with advanced security features, monitoring, and enterprise management controls;
- Execution of a scalable, enterprise cybersecurity contract to consolidate operating administration (OA) contracts, and streamline, and improve the implementation and operation of DOT's cybersecurity program, thereby improving the consistency of cybersecurity-related services and outcomes; and,
- Modernization of the Department's enterprise web vulnerability scanning solution to improve scalability, performance, and resilience so that DOT and OA personnel can rely on the solution for the assessment of web sites and applications.

Cybersecurity will continue to be a priority for DOT, with increased attention from agency leadership, and efforts both direct, and indirect, to reduce risks across the enterprise, increase resilience in support of the agency mission, and improve internal controls through enhanced, integrated management of IT. We look forward to sharing the results of our efforts with the OIG during FY 2019.

Upon review of the OIG draft report we concur with the 12 recommendations and will complete planned actions by September 30, 2020.

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 IG 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