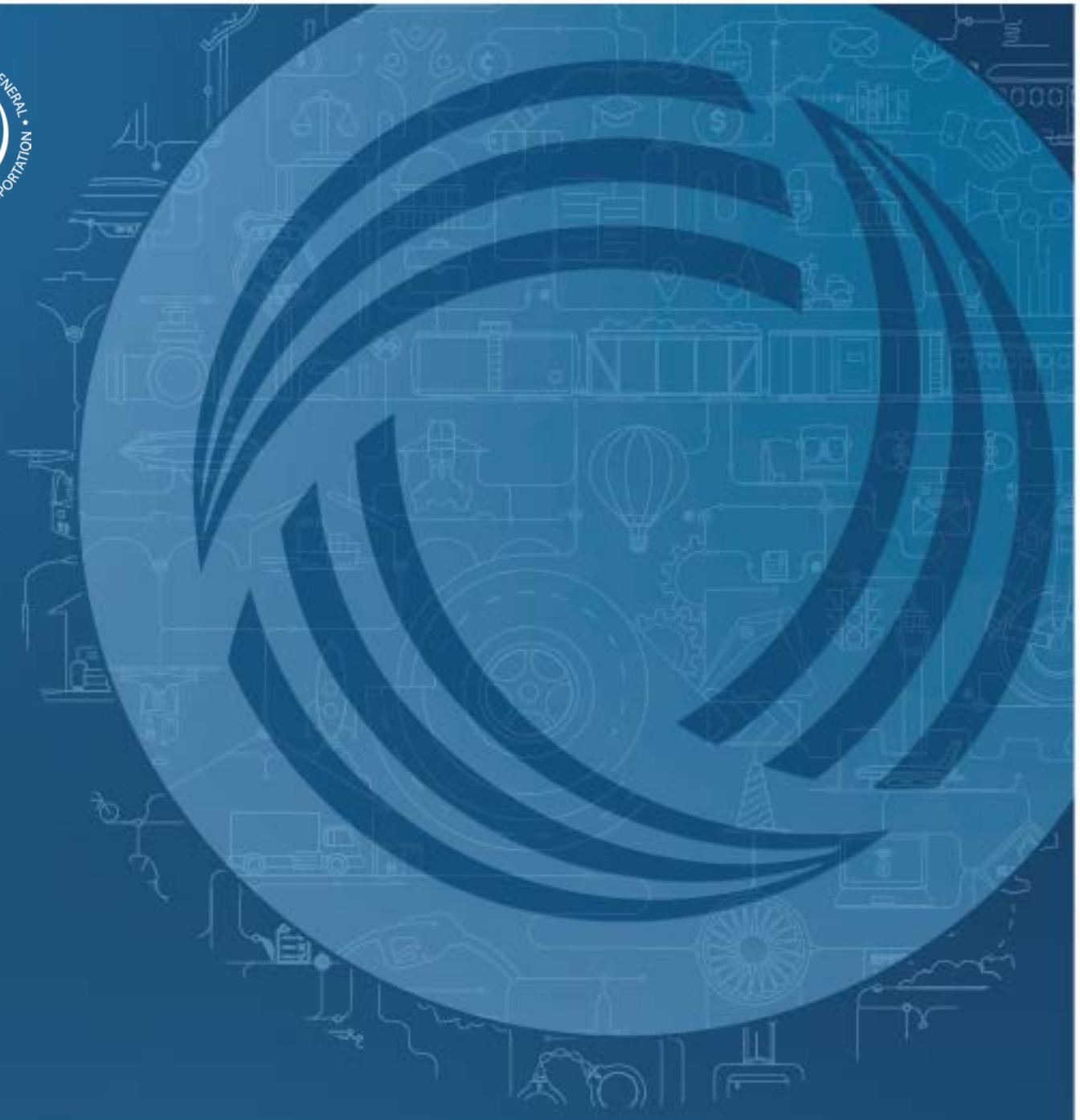

OST

Report QC2022006
October 25, 2021

Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices

Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices

Required by the Federal Information Security Modernization Act of 2014

Office of the Secretary of Transportation | QC2022006 | October 25, 2021

What We Looked At

This report presents the results of our quality control review (QCR) of an audit of the Department of Transportation's (DOT) information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, implement, and document agencywide information security programs and practices. FISMA also requires inspectors general to conduct annual reviews of their agencies' information security programs and report the results to the Office of Management and Budget.

To meet this requirement, we contracted with CliftonLarsonAllen LLP (CLA) to conduct this audit subject to our oversight. The audit objective was to determine the effectiveness of DOT's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

We performed a QCR of CLA's report and related documentation. Our QCR disclosed no instances in which CLA did not comply, in all material respects, with generally accepted Government auditing standards.

Recommendations

DOT concurs with all five of CLA's recommendations. CLA considers all five recommendations resolved but open pending completion of planned actions.

Contents

U.S. Department of Transportation
Office of Inspector General

Memorandum

Date: October 25, 2021

Subject: INFORMATION: Quality Control Review of the Independent Service Auditor's Report on DOT's Information Security Program and Practices | Report No. QC2022006

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Chief Information Officer

The Federal Information Security Modernization Act of 2014 (FISMA) requires agencies to develop, implement, and document agencywide information security programs and practices. FISMA also requires inspectors general to conduct annual reviews to determine the effectiveness of their agencies' information security programs and report their review results to the Office of Management and Budget. To meet this requirement, we contracted with CliftonLarsonAllen LLP (CLA), an independent public accounting firm, to conduct this audit subject to our oversight.

The audit objective was to determine the effectiveness of DOT's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

CLA found that DOT's information security program is at the Defined maturity level—the second lowest level in the maturity model for information security programs. As a result, DOT's program is not effective. CLA made the following recommendations to the Chief Information Officer (CIO) to help DOT develop a mature and effective information security program:

1. Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.

2. Undertake a strategic analysis of the Inspector General FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy and approach to include objective milestones, and resource commitments by the Department and the CIO that address the corrective actions

necessary to show steady, measurable improvements towards an effective information security program.

3. Work with the Federal Aviation Administration's CIO and Federal Motor Carrier Safety Administration's Information Security System Manager (ISSM), to investigate and remediate cross-site scripting vulnerabilities identified in public facing web applications.

4. Work and coordinate with system owners to identify and remediate weak and default authentication mechanisms within their systems and the Common Operating Environment.

5. Develop and implement a process to facilitate centralized monitoring, oversight (by ISSMs and their alternates) and escalation efforts to ensure the timely completion of required security awareness training and role based training for all DOT personnel leveraging an automated integrated solution(s) and dashboards.

We performed a QCR of CLA's report, dated September 30, 2021 (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement and performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on DOT's information security program and practices. CLA is responsible for its independent auditor's report and the conclusions expressed in that report. Our QCR disclosed no instances in which CLA did not comply, in all material respects, with generally accepted Government auditing standards.

We appreciate the courtesies and cooperation of DOT representatives during this engagement. If you have any questions concerning this report, please call me at (202) 366-1518.

cc: The Secretary
Deputy Secretary
DOT Audit Liaison, M-1

Agency Comments and OIG Response

On August 20, 2021, CLA provided DOT with its draft report and received DOT's response on September 20, 2021. DOT's response is included in its entirety as part of the attached independent auditor's report. DOT concurred with all five of CLA's recommendations and provided appropriate planned actions and estimated completion dates.

Actions Required

We consider all five recommendations resolved but open pending completion of planned actions.

Exhibit. List of Acronyms

CIO	Chief Information Officer
CLA	CliftonLarsonAllen, LLP
DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act
ISSM	Information Security System Manager
QCR	Quality Control Review

Attachment. Independent Auditor's Report

U.S. Department of Transportation's 2021 Federal Information Security Modernization Act of 2014 Audit

Final Report

September 30, 2021

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

phone 571-227-9500 **fax** 571-227-9552
CLAconnect.com

September 30, 2021

Kevin Dorsey
Assistant Inspector General for Information Technology Audits
U.S. Department of Transportation
Office of the Inspector General
1200 New Jersey Ave, SE
Washington, D.C. 20590

Dear Mr. Dorsey:

CliftonLarsonAllen LLP (CLA) is pleased to present our performance audit report on the U.S. Department of Transportation's (DOT or the Department) information security management program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Federal Information Security Modernization Act of 2014 (FISMA) for the twelve months ending on June 30, 2021.

We appreciate the assistance we received from DOT. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
United States Department of Transportation

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the U.S. Department of Transportation's (DOT or the Department) information security management program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Federal Information Security Modernization Act of 2014 (FISMA or Act) for the twelve months ending on June 30, 2021. FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual review of their agencies' information security programs and report the results to the Office of Management and Budget (OMB).

For fiscal year (FY) 2021, OMB required IGs to assess 66 metrics in five 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. The maturity levels range—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, including its performance in the five security function areas for the 12 months ending on June 30, 2021.

Our audit was performed in accordance with GAGAS. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To address OMB's 2021 FISMA reporting metrics, we reviewed select controls for a sample of 63 DOT FISMA reportable systems, performed an internal and external vulnerability assessment and penetration test, interviewed Department officials, and reviewed data, including system security and privacy documentation. Refer to Appendix A for background on the FISMA legislation and Appendix B for details on our scope and methodology. We also reviewed the status of the 69 open FISMA prior year recommendations related to DOT's security program and practices. Appendix C contains the current year status of prior FISMA report recommendations. Appendix D lists the organizations we visited or contacted during our audit. Appendix E provides a listing of the representative subset of sampled systems. Appendix F provides a listing of acronyms used throughout this report and Appendix G contains management comments to the report.

Based upon our audit of DOT's information security program, including its performance in the function areas, we concluded that overall, DOT is at the Defined maturity level – the second lowest level in the maturity model for an information security program, and thus not effective. Specifically, four functional areas achieved a maturity level of Defined (Level 2) with one functional area achieving a Consistently Implemented (Level 3) maturity level for an overall maturity level of Defined for the security program. The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT continues to face significant challenges in the consistent implementation of its information security program across the

Department. In addition, controls need to be applied in a comprehensive manner to information systems across DOT in order to be considered consistent and fully effective by achieving at least a rating of Level 4, *Managed and Measurable*.

Accordingly, there are longstanding security deficiencies similar in type and risk level to prior years and an overall inconsistent implementation of the security program. Consequently, we noted weaknesses in eight of the nine IG FISMA Metric Domains encompassing the Department's Agency-wide program. The audit identified continuing deficiencies related to risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction. Many of these weaknesses can be attributed to an inconsistent enforcement of an agency-wide information security program across the enterprise, ineffective communication between the Department and the Operating Administrations, and the lack of progress in the remediation of prior year audit recommendations.

We made 5 new recommendations to help the Department address challenges in its development of a mature and effective information security program. The new recommendations include a recommendation for DOT to undertake a strategic analysis of the IG FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy and approach to include objective milestones, and resource commitments by the Department and the Chief Information Officer that addresses the corrective actions necessary to show steady, measurable improvements towards an effective information security program. In addition, we noted 66 recommendations related to prior FISMA audits are still open.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on August 13, 2021. We have no obligation to update our report or to revise the information contained herein to reflect events occurring subsequent to August 13, 2021.

The purpose of this audit report is to report on our assessment of DOT's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations is included in the accompanying report.

CliftonLarsonAllen LLP

Arlington, Virginia
September 30, 2021

Table of Contents

Executive Summary

The Federal Information Security Modernization Act of 2014[1] (FISMA) requires Federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and information systems, including those provided or managed by another Agency, contractor, or other source. FISMA also requires Agency Inspectors General (IGs) to assess the effectiveness of Agency information security programs and practices. Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for Federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards (FIPS) to establish Agency baseline security requirements.

The U.S. Department of Transportation (DOT or the Department) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct an audit in support of the FISMA requirement for an annual audit of DOT's information security program and practices. The objective of this performance audit was to determine the effectiveness of DOT's information security program, including its performance in five function areas – Identify, Protect, Detect, Respond and Recover.[2]

FISMA requires us to assess the maturity of five functional areas in DOT's information security program and practices. This assessment used objective metrics that are standardized across the Federal government. To be considered effective, an Agency's information security program must be rated *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5).

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Audit Results

DOT's overall information security program and the effectiveness of its security program and practices in accordance with FISMA did not meet the requirements to be considered effective. Based upon our audit of DOT's information security program, including its performance in the function areas, we concluded that overall, DOT is at the Defined maturity level – the second lowest level in the maturity model for an information security program, and thus not effective. Specifically, four functional areas achieved a maturity level of Defined (Level 2) with one functional area achieving a Consistently Implemented (Level 3) maturity level for an overall maturity level of Defined for the security program as noted in **Table 1** below.

[1] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] The fiscal year (FY) 2021 metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 1: FY 2021 IG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions[3]	FY 2021 Maturity Level by Function	Metric Domains	Domain Maturity Level
Identify	Defined (Level 2)	**Risk Management**	Defined (Level 2)
		Supply Chain Risk Management[4]	Ad Hoc (Level 1)
Protect	Defined (Level 2)	**Configuration Management**	Defined (Level 2)
		Identity and Access Management	Defined (Level 2)
		Data Protection and Privacy	Defined (Level 2)
		Security Training	Defined (Level 2)
Detect	Defined (Level 2)	**Information Security Continuous Monitoring**	Defined (Level 2)
Respond	Consistently Implemented (Level 3)	**Incident Response**	Consistently Implemented (Level 3)
Recover	Defined (Level 2)	**Contingency Planning**	Defined (Level 2)
Overall	**Level 2: Defined - Not Effective**		

The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT continues to face significant challenges in the consistent implementation of its information security program and monitoring of security controls across the Department. In addition, controls need to be applied in a comprehensive manner to information systems across DOT in order to be considered consistent and fully effective by achieving at least a rating of Level 4, *Managed and Measurable*.

Accordingly, there are longstanding security deficiencies similar in type and risk level to findings in prior years and an overall inconsistent implementation of the security program. Consequently, we noted weaknesses in eight of the nine IG FISMA Metric Domains encompassing the Department's Agency-wide program. The audit identified continuing deficiencies related to risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction. Many of these weaknesses can be attributed to an inconsistent enforcement of an agency-wide information security program across the enterprise, ineffective communication between the Department and the Operating Administrations (OAs), and the lack of progress in the remediation of prior year audit recommendations.

[3] See Table 3 and Table 4 in Appendix A for definitions and explanations of the Cybersecurity Framework Security Functions and FISMA Metric Domains and Maturity Levels, respectively.
[4] This domain will not be considered in the Identify framework function rating for FY2021.

This lack of progress is also attributed to DOT not having a permanent Chief Information Security Officer (CISO) assigned with information security responsibilities as their primary role,[5] as required by the FISMA Act.[6] Additionally, with the volatility in leadership tenure in the Chief Information Officer (CIO) position, it is challenging for DOT to move forward with any continuity of strategy and momentum to affect long term changes to DOT's information security program. Considering that agency heads often exclusively rely upon the CIO and the CISO for matters of information security, by not having a permanent CISO and CIO detracts from needed leadership, oversight, and accountability necessary for agency-wide improvements to address ongoing information security program weaknesses.

Furthermore, despite repeated auditor requests, no closure packages were provided by the Department to demonstrate achievement or major steps taken towards remediating the prior open FISMA audit recommendations. Specifically, there are currently 66 open FISMA audit recommendations[7] going back to fiscal year (FY) 2010, which demonstrates that DOT has not gained momentum in addressing the underlying root causes of these recurring security weaknesses.

In order to demonstrate measurable improvements towards an effective information security program, the Department needs to improve its performance monitoring to ensure controls are operating as intended for all systems and at all OAs. Additionally, DOT needs to communicate security deficiencies to the appropriate personnel, who should take responsibility for developing corrective actions and ensuring those actions are implemented. The Department also needs to ensure adequate resources are assigned to support the CISO's office to include a permanent CISO official with information security as their primary duty, and to ensure compliance with DOT's information security policies and procedures. Furthermore, the Department needs to complete an analysis of the IG FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy to include objective milestones, and resource commitments by the Department and the CIO that addresses the corrective actions necessary to show steady, measurable improvements towards an effective information security program.

At present, the weaknesses that we identified (as summarized in **Table 2** below) leave DOT operations and assets at risk of unauthorized access, misuse, and disruption. Although the majority of these weaknesses were similar to prior year reported weaknesses, with corresponding recommendations remaining open, we made 5 new recommendations to help the Department address challenges in its development of a mature and effective information security program. In addition, 66 prior FISMA recommendations related to DOT's information security program and practices remain open.

Most importantly, we recommend DOT undertake a strategic analysis of the IG FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy and approach to include objective milestones, and resource commitments by the Department and the CIO that addresses the corrective actions necessary to show steady, measurable improvements towards an effective information security program. Implementing such a plan will require DOT to allocate sufficient resources, including staffing, and to be accountable for interim milestones, in order to reach an overall effective rating within a reasonable period to be specified by management.

[5] During the past year, the CISO was serving in an acting capacity in addition to serving as the Associate CIO of Strategic Portfolio Management, until a permanent CISO is hired.
[6] FISMA Act of 2014, § 3554. Federal agency responsibilities, A(iii).
[7] See Appendix C for status of recommendations from the OIG's prior FISMA audits.

Table 2: FY 2021 IG FISMA Metric Domains mapped to weaknesses noted in FY 2021 FISMA Audit

FY 2021 IG FISMA Metric Domains	Weaknesses Noted in 2021
Risk Management	Plan of Action and Milestones (POA&Ms) and information security weaknesses were not effectively managed.
	Security Assessment and Authorization (SA&A) documentation was not properly approved, controls were not tested or scheduled for testing, or security documentation was outdated or did not exist.
	The system inventory maintained in Cybersecurity Assessment and Management System (CSAM) was not accurate.
	System hardware inventories were unable to be reconciled.
Supply Chain Risk Management	A supply chain risk management strategy or plan has not been developed.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Configuration management plans and policies were not consistently maintained.
	Change management procedures were not consistently followed for system changes.
Identity and Access Management	Incomplete deployment of two-factor user authentication mechanisms.
	System access was not effectively documented, and rules of behavior, access requests and approvals were lacking.
	Background reinvestigations were not performed timely.
Data Protection and Privacy	Privacy Threshold Assessments (PTAs), and Privacy Impact Assessments (PIAs) were either not completed or updated.
Security Training	Security training requirements were not fully implemented.
Information Security Continuous Monitoring	Information security continuous monitoring of controls and assessment plans were not properly completed, provided, or performed annually.
Contingency Planning	Contingency plans were either out of date, incomplete, or missing for some systems.
	Contingency plans were not tested in a timely manner for some systems.
	Business Impact Analysis (BIAs) were not developed for some systems.

The following section provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions. Appendix A describes background information on the FISMA legislation. Appendix B describes the audit scope and methodology. Appendix C contains the current year status of prior FISMA report recommendations. Appendix D lists the organizations visited or contacted during our audit. Appendix E provides a listing of the representative subset of sampled systems. Appendix F provides a listing of acronyms utilized throughout this report and Appendix G contains management comments to the report.

FISMA Audit Findings

Security Function: Identify

Overview

DOT developed and published the DOT *Cybersecurity Compendium* in 2018 to describe its entity-wide information security risk management program and Risk Management Framework (RMF). The RMF addresses both security and privacy controls. DOT's information security risk management process focused on identifying and evaluating the threats and vulnerabilities to DOT information. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. However, DOT's risk management process was not fully effective since gaps and inconsistent implementation of the policies and procedures continue to exist.

Metric Domain – Risk Management

FISMA requires each Federal Agency to develop, document, and implement an Agency-wide information security and risk management program. Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, agencies should assess the likelihood that an event will occur and the resulting impact. With this information, agencies can determine the acceptable level of risk for delivery of services and can set their risk tolerance.

DOT has not fully implemented components of its Agency-wide information security risk management program to meet FISMA requirements. The policies, procedures, and documentation included in the DOT enterprise risk management program were not consistently implemented or applied across all DOT systems. Specifically, we identified weaknesses not tracked within a risk management program (e.g., POA&Ms), POA&Ms which missed key milestone dates, POA&Ms with incomplete data, POA&Ms not reviewed quarterly and improper closure of POA&Ms. In addition, SA&A documentation was not properly approved, controls were not tested or scheduled for testing, and security documentation was outdated or did not exist.

We also identified system inventory weaknesses, including OA system inventory listings not consistently aligning with the official Department system inventory maintained in CSAM.[8] In addition, hardware inventory data reported within the Office of the Chief Information Officer (OCIO) FISMA Metrics was unable to be reconciled to supporting artifacts provided by the OAs and the Department.

National Institute of Standards and Technology (NIST) Special Publications (SP) 800-37, Revision 2, *Risk Management Framework to Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* is guidance for applying the RMF controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The goal of the RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

[8] The Department's main repository for tracking system inventories, security assessment and authorization documentation, weaknesses, and other system security information.

The following details the weaknesses noted in DOT's risk management framework.

Plan of Action and Milestones:

OMB Memorandum M-02-01*, Guidance for Preparing and Submitting Security Plans of Action and Milestones*, defines management and reporting requirements for Agency POA&Ms, to include deficiency descriptions, remediation actions, required resources, and responsible parties. In addition, POA&Ms identify what actions must be taken to remediate system security risks and improve DOT's overall information security posture.

However, we noted that POA&Ms were not effectively managed throughout the Department. According to DOT's central reporting database, CSAM, the Department had approximately, 10,663 open POA&Ms as of June 30, 2021, as compared to 10,385[9] open POA&Ms in 2020. Of the total number of open POA&Ms, 9,940 or 93 percent are under the FAA. This large number of open POA&Ms for FAA reflects ongoing efforts to migrate, integrate, and reconcile FAA security control weaknesses into CSAM from another system.

In addition, for the sample of DOT systems tested, we identified deficiencies related to reporting, managing and closing of POA&Ms. Specifically, we identified: (a) POA&Ms not consistently established or updated to consider all known security weaknesses; (b) action items that missed major milestone dates and were not updated to accurately reflect their current status; (c) POA&Ms that were missing attributes and details, such as cost requirements; d) POA&Ms which were not reviewed/updated at least quarterly and (e) POA&Ms that lacked sufficient documentation to justify closure, or closure was not performed by the proper individual. Specifically, we identified the following POA&M weaknesses for the sample of systems tested:

- For 24 of 63[10] sampled systems, or 38 percent, POA&Ms were not consistently established for controls that were identified as non-compliant during Security Control Assessments (SCAs). (18 FAA systems, 1 FRA system, 1 FTA system, 1 OIG system, 1 OST I&O[11] COE system, and 2 OST systems).[12]
- For 20 of 25 sampled open POA&Ms, or 80 percent, open POA&Ms either missed scheduled completion dates without updates or justifications, or were established with missing details, such as cost requirements. (11 FAA systems, 1 OIG system and 1 OST system).
- For 12 of 25 sampled open POA&Ms, or 48 percent, POA&Ms were not reviewed at least quarterly in accordance with DOT policy.[13] (For 9 FAA systems, 1 MARAD system, and 1 OST system).
- For 23 of 25 sampled closed POA&Ms, or 92 percent, POA&Ms were not closed by an individual serving in an oversight role, in accordance with DOT policy.[14] (1 NHTSA system, 4 OST systems, 1 FAA system and 1 FMCSA system).

[9] FISMA 2020: *DOT's Information Security Program and Practices* (DOT OIG Report Number QC2021003, October 26, 2020).
[10] DOT's population of systems includes 447 FISMA reportable systems as of February 1, 2021. For the purposes of this audit and our sample system selection, we have excluded all systems that had a response in the "System Type" field other than "Major Application" or "General Support System". This resulted in a population of 431 systems. From this population, we obtained a sample of systems randomly from each of 15 combinations of OAs and risk stratification, resulting in a sample size of 63 systems.
[11] I&O stands for Infrastructure and Operations, which was previously called IT Shared Services or ITSS.
[12] These represent OAs in which described weaknesses were identified. Refer to Appendix D for OA acronyms and descriptions.
[13] *DOT Security Weakness Management Guide*, January 2020, version 4.0, section 3.3.1.
[14] *DOT Security Weakness Management Guide*, January 2020, version 4.0, section 3.4.

- For 6 of 25 sampled closed POA&Ms, or 24 percent, POA&Ms were closed without sufficient justification or evidence to support the remediation of weaknesses (1 NHTSA system, 1 OST system and 1 FMCSA system).
- 7 FAA Air Traffic Operations (ATO) in scope systems did not maintain their official and up to date POA&M listing within CSAM, the official DOT repository. Another repository was utilized, with CSAM updated on an ad hoc basis.

DOT Policy[15] requires each POA&M item to be completed with DOT mandatory fields, including but not limited to status, estimated cost, scheduled and actual completion dates, milestones, and milestone changes. OCIO did not enforce requirements for ensuring the development, monitoring and timely remediation of weaknesses. In addition, management did not ensure DOT policy was followed for the management of POA&Ms or that FAA fully utilized CSAM as the official POA&M document repository.

Incomplete information on POA&Ms in CSAM inhibits the CIO and CISO to assess risk and funding requirements, analyze weakness trends, and implement department-wide solutions. Without sufficient documentation to justify closure of POA&Ms, DOT cannot ensure that corresponding security risks have been fully mitigated. In addition, without properly managing POA&Ms, DOT is at risk of not adequately tracking or remediating operating systems and applications with known security weaknesses.

Security Assessment and Authorization

SA&A documentation was not effectively managed throughout the Department. As a result of system owners not effectively managing their systems and complying with DOT policies, for the sample of DOT systems within scope across the OAs, we noted weaknesses related to the creation, maintenance, monitoring, and retention of SA&A documentation. Departmental policy[16] requires OAs to annually assess security controls for their information systems and operating environments and examine the following security documentation: system security plan, security assessment report, and security assessment plan. However, we noted the following weaknesses related to SA&A processes:

- For 14 of the 63 sample systems, or 22 percent, the Authorization to Operate (ATO) was either expired, not authorized by the appropriate Authorizing Official (AO), the AO was not consistently listed across the system security plan (SSP), ATO and Designation of Authorizing Official memorandum, or not provided. Based on our sample, we estimate 98 of 431[17] systems, or 22.8 percent,[18] have an ATO that is either expired, not authorized or consistently listed by the appropriate AO, or not available (FAA, FHWA, MARAD, and OST I&O COE).

[15] DOT *Cybersecurity Compendium Supplement to DOT Order 1351.37 v4.2,* May 2018.
[16] DOT *Security Authorization & Continuous Monitoring Performance Guide*, September 2019, version 4.2 and FAA (FY21) Security Authorization Handbook, December 2020, version 1.
[17] DOT's population of systems includes 447 FISMA reportable systems as of February 1, 2021. For the purposes of this audit and our sample system selection, we have excluded all systems that had a response in the "System Type" field other than "Major Application" or "General Support System". This resulted in a population of 431 systems.
[18] Our 22.8 percent estimate has a margin of error of +/- 9.3 percentage points at the 90 percent confidence level.

- For 13 of 63 sample systems, or 20.6 percent, SSPs did not include all required attributes, were not current or updated annually, or were not provided. Based on our sample, we estimate 80 of 431 systems, or 18.5 percent,[19] have SSPs that were not current or updated annually, did not include all required attributes, or could not be provided (FAA, MARAD, NHTSA and OST I&O COE).
- For 9 of 63 sample systems, or 14.3 percent, SCAs were not performed annually, or were not provided. Based on our sample, we estimate 66 of 431 systems, or 15.2 percent,[20] did not perform SCAs annually, or could not provide evidence a SCA was completed (FAA, FMCSA, and MARAD).
- For 12 of 63 sample systems, or 19 percent, the FIPS 199 categorizations did not align with the overall rating listed within the SSP and system characterization document (SCD), or were not provided. Based on our sample, we estimate 84 of 431 systems, or 19.5 percent,[21] did not have FIPS 199 categorizations consistently listed, or were not provided (FAA, FRA[22] and MARAD).
- For 17 of 63 sample systems, or 27 percent, risk assessments (as documented within a Security Assessment Report (SAR)) did not include the likelihood, impact, and mitigation, were not current, were expired, or were not provided. Based on our sample, we estimate that 103 of 431 systems, or 23.8 percent[23], did not provide risk assessments, they were outdated or were missing key attributes. (FAA, FMCSA, MARAD, OST, OST I&O COE, and PHMSA).

These weaknesses were attributed to a combination of reasons including pandemic restrictions affecting system decommissioning processes; SA&A documentation permitted to lapse during system decommissioning; management oversight; third party assessors not required to include all SA&A documentation within DOT deliverables; and an incorrect reliance upon other documents such as relying upon security plans in lieu of a system characterization or risk assessment document.

Additionally, the Department did not have a multi-year strategy and approach in place for addressing long standing FISMA weaknesses to demonstrate steady, measurable improvements towards an effective information security program such as in the management of SA&A documentation.

Without assessing the effectiveness of security controls on a continuous basis, DOT does not have assurance that controls are operating effectively, and this may expose the Department to information loss, fraud, or abuse. In addition, the 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.

[19] Our 18.5 percent estimate has a margin of error of +/- 8 percentage points at the 90 percent confidence level.
[20] Our 15.2 percent estimate has a margin of error of +/- 7.4 percentage points at the 90 percent confidence level.
[21] Our 19.5 percent estimate has a margin of error of +/- 8.1 percentage points at the 90 percent confidence level.
[22] A SCD was subsequently provided by FRA, however after our audit period, with a July 2021 creation date.
[23] Our 23.8 percent estimate has a margin of error of +/- 8.7 percentage points at the 90 percent confidence level.

Comprehensive Information System Inventory

DOT policies and procedures state that the Department will maintain an inventory of information systems operated by or under its control deemed reportable to OMB for FISMA.[24] DOT did not maintain a complete and accurate inventory of all its information systems by OA. Inventory listings provided by the OAs did not consistently align with the department-wide system inventory listing within CSAM or align with OCIO FISMA Metrics submissions.

For example, two FRA systems[25] were included in the Department CSAM inventory but were not included in the respective OA system inventory. We also noted four FHWA systems, one FMCSA and two FTA systems were included in the OA cloud system inventory but were not included in the Department cloud inventory. We noted one MARAD system was included in the Department cloud inventory; however, not in the OA cloud inventory. In addition, we noted that the OCIO FISMA Metrics had listed one FHWA, four FAA, one FRA, one PHMSA and three OST cloud systems; however, not included in the Department cloud inventory. Also, 29 cloud systems were listed in the Department cloud inventory; however, not listed in the OCIO FISMA Metrics submitted to OMB.

The Department Acting CISO indicated that the CSAM inventory is the official system inventory for the Agency, and no other entity outside of the DOT CISO can provide the official inventory, and component-level inventories outside of CSAM are not considered authoritative. However, as described above, we noted that the OAs (the source of determining the accuracy and completeness of their own system inventory and who utilize and are responsible for managing and updating their inventory in CSAM) were also maintaining inventories outside of CSAM and their inventory records did not reconcile to the Department system inventory. The Department considers CSAM to be the official system of record for system inventory and all necessary updates will follow the DOT FISMA Inventory Guide. Therefore, the Department considers that any additional system inventory information provided to the components is not valid and thus there is no need to reconcile or investigate any noted discrepancies. This lack of oversight by DOT has not ensured a comprehensive and accurate inventory of its information systems is maintained by periodically reconciling CSAM to the different OA system inventory listings and investigating discrepancies.

The absence of a complete and accurate inventory of all information systems creates a risk that the Department may not be aware of all systems in its environment and be able to identify and address all existing vulnerabilities.

Asset Inventory

NIST standards[26] require DOT to develop and document a comprehensive inventory of information system components that accurately reflects the current information systems, includes all components within the authorization boundary of the system, and is at the level of granularity deemed necessary for tracking and reporting. OAs are required per DOT policy,[27] to provide quarterly updates to OCIO on the current inventory for overall reporting to OMB.

[24] DOT's *FISMA Inventory Guide*, Version 1.1, dated September 2013.
[25] For the two FRA systems which were not included in the FRA system inventory listing from March 2021, management in a response subsequent to this finding indicated these systems were in development status at the time.
[26] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015 – security control, CM-8 Information System Component Inventory.
[27] DOT *Cybersecurity Compendium Supplement to DOT Order 1351.37 v4.2,* May 2018 - CM-8.

However, OCIO was unable to demonstrate a formalized process is in place to ensure the accuracy and completeness of hardware asset inventories reported to OMB within the CIO FISMA Metrics, through the reconciliation of manually collected, point-in-time data against real-time data produced by the associated systems and capabilities. Specifically, hardware asset inventory counts reported in the FY2021 Quarter 1 and Quarter 2 CIO FISMA Metrics submissions, were unable to be reconciled to Department hardware asset inventory spreadsheets or other subordinate inventory artifact listings provided.

Since the Department's efforts to automate Continuous Diagnostic and Mitigation (CDM) and other programs and services is an ongoing effort, they have experienced challenges in reconciling manually collected, point-in-time data (*using asset inventories maintained outside of BigFix*)[28] against real-time data (*e.g., BigFix*) produced by current systems and capabilities.

As a result, DOT may not be aware of all assets residing in its environment and therefore may not be appropriately managing and protecting all assets.

Metric Domain – Supply Chain Risk Management

FISMA requires each Federal Agency to develop, document and implement Agency-wide strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. As noted in the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks.

DOT has not developed and communicated an organization wide Supply Chain Risk Management (SCRM) strategy and implementation plan to manage supply chain risks. Although DOT has taken several actions to address SCRM risks, a comprehensive SCRM strategy has not yet been developed. Actions taken to date include: Section 889 contractual clause requirements and related training; limited references to SCRM within the *Security Authorization & Continuous Monitoring Performance Guide* and utilizes configuration change boards to evaluate risks present in new technology solutions. Additionally, OCIO performs ad-hoc reviews of IT spend, acquisitions, and OA deployments as part of its IT Spend approval processes and enterprise change management process.

The lack of an overall SCRM strategy, can be partly attributed to ongoing efforts by DOT to develop a department level assessment of risk appetite and tolerance related to enterprise risk management which is integrated with the IT Enterprise risk management plan. However, DOT is still awaiting further implementation directions from OMB and Department of Homeland Security (DHS) to outline the process to address supply chain risk management strategy/action plans and related policy and procedural requirements of the SECURE Technology Act.[29] Additionally, we understand that DOT's SCRM program has been reviewed by the Government Accountability Office (GAO), and the Department is in the process of implementing actions in response to related recommendations.

[28] BigFix is an endpoint management platform that allows continuous configuration compliance, patch deployment, and vulnerability remediation and monitoring.

[29] Public Law 115 - 390 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act' or the "SECURE Technology Act."

Recommendations:

We recommend that the DOT CIO take the following actions, in addition to addressing the prior open recommendations[30] related to the weaknesses noted for the Identify function:

1. Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.
2. Undertake a strategic analysis of the IG FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy and approach to include objective milestones, and resource commitments by the Department and the CIO that addresses the corrective actions necessary to show steady, measurable improvements towards an effective information security program.

[30] Prior FISMA open recommendations related to the findings noted within the "Identify" function: Recommendations 2, 8, and 9 (DOT OIG Report # FI-2016-001, 11/5/2015); Recommendations 1, 2, 5, and 6 (DOT OIG Report # FI-2017-008, 11/09/2016); Recommendations 3 and 9, (DOT OIG Report Number FI-2019-023, 3/20/2019); and Recommendations 1, 2, 3, and 4 (DOT OIG Report Number QC2020002, 10/23/2019). These recommendations are not being repeated within this report. Refer to Appendix C for details on these recommendations.

Security Function: Protect

Overview

DOT's Protect controls which cover configuration management, identity and access management, data protection and privacy, and security training were not effective and not consistently implemented across the Department. In FY 2021, weaknesses in the DOT IT environment continue to contribute to deficiencies in system configuration, data protection and privacy, access controls, and security training.

Metric Domain – Configuration Management

To secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. Furthermore, NIST has developed a repository of secure baselines for a wide variety of operating systems and devices. In addition, configuration management policies and plans should be current with documented configuration management processes, and change requests documented, properly approved, and tested.

OCIO does not enforce OMB's requirements[31] for addressing weaknesses in configuration management. We identified deficiencies in configuration management controls, designed to ensure DOT's critical systems have appropriate security baselines, current and vendor supported operating systems, accurate system and software inventories, and up-to-date vulnerability patches. DOT policy[32] provides policies on mandatory configuration settings for information technology hardware, software, and firmware. DOT has not consistently implemented vulnerability remediation and management processes. Unsupported operating systems, unpatched applications and configuration weaknesses existed without adequate protection.

Independent vulnerability and penetration testing assessments of DOT's COE and a sample of systems identified critical and high-risk vulnerabilities related to patch management, configuration management, and unsupported software that may allow unauthorized access into mission critical systems and data. Many of these vulnerabilities have existed since they were first identified in the FY 2019 FISMA audit. Due to the vulnerabilities identified, the assessment team was able to exploit certain vulnerabilities.

An attacker may exploit the vulnerabilities identified to take control over certain systems, cause a denial-of-service attack, or gain unauthorized access to critical files and data. In addition, the inconsistent application of vendor patches could jeopardize the data integrity and confidentiality of DOT's sensitive information. Without remediating all significant security vulnerabilities, systems could be compromised, resulting in potential harm to data confidentiality, integrity, and availability.

<u>Configuration Management Plans</u>

To facilitate the implementation of configuration management policy and associated configuration management controls, the DOT *Departmental Cybersecurity Compendium*, specifically control DOT CM-9 Configuration Management Plan, requires every DOT information system owner to develop a configuration management plan which identifies and manages different types of

[31] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (2013).
[32] *DOT Security Weakness Management Guide,* January 2020.

configuration items, and defines configuration items for the information system and places them under configuration control.

We noted weaknesses in the effectiveness of Configuration Management Plans for FAA, OST I&O, and FMCSA systems. These plans were either not current, not provided, or were missing key components (such as roles and responsibilities, defined configuration items subject to change control, explicit consideration of security impacts of changes, or fully defined configuration change control activities). In addition, the FAA Order 1800.66, *Configuration Management Policy*, dated 3/12/2012, is currently undergoing revisions and is not aligned with the Electronic Industries Alliance (EIA)-649, *National Consensus Standard for Configuration Management*, the industry consensus standard for configuration management.

This situation arose because the OAs believed that a) it was not efficient to have separate configuration management plans for each system, since these were reliant upon the I&O Change Control Board (CCB) or FAA change processes, or b) due to ongoing system consolidation efforts, OAs were awaiting completion of these efforts before developing and/or updating plans.

If configuration management policies and plans are not current and configuration management processes are not documented, DOT's ability to adequately secure and protect its information systems could be affected and those systems and the Department could be at risk for compromise.

Change Management Procedures

To facilitate the implementation of configuration change control policy and associated configuration change controls, the DOT *Departmental Cybersecurity Compendium*, specifically controls CM-3 Configuration Change Control and CM-4 Security Impact Analysis, requires every information system owner to implement changes that are approved by the Technical Configuration Control Board (TCCB) only, to ensure any proposed changes are tested, validated, and documented before the change is implemented into production, and to analyze the security impact before implementing changes to any information system.

Weaknesses were noted in the effectiveness of FAA and OST I&O change management controls based on the testing results for a selection of 25 changes made to 8 FIPS 199 high risk systems. These weaknesses included missing approvals; missing test plans, missing evidence of test results, a security impact analysis, or a post implementation audit of the configuration change request(s).

These weaknesses were attributed to either an inconsistency between change management plan requirements and actual implementation or inadequate monitoring and oversight of implemented changes.

Without adherence to proper change management procedures, including security impact analysis, changes may be moved into production with inadequate knowledge or consideration of their related effects on system risk and security controls in place for affected systems. In addition, without documented test plans and results, changes may not address management's needs, expectations, commitments, and system requirements appropriately or may not function as intended/create unintended consequences upon approval for release to production. Further, without evidence of post implementation audits of change/configuration requests, DOT may be

unable to verify whether the change fully solved the problem it was designed to address, whether data integrity was maintained after the change or whether proper approvals were tracked and maintained for each change.

Metric Domain – Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized and authenticated to access information and information systems. In addition, policy and procedures must be in place for the creation, provisioning, maintenance, and eventual termination of accounts. Homeland Security Presidential Directive 12 calls for all Federal departments to require personnel to use personal identity verification (PIV) cards as a major component of a secure, government-wide account and identity management system. Also, prior to obtaining access to DOT systems, personnel are required to receive a background investigation, which is to be re-performed every several years in accordance with DOT policies, such as DOT 1630.2C, *Personnel Security Management*.

User Authentication

OMB M-11-11[33] required that, by FY 2012, all Federal employees and contractors use PIV cards to log into Agency computers and system applications as a part of multifactor authentication. Additionally, Agencies shall require PIV credentials (where applicable in accordance with Office of Personnel Management (OPM) requirements) as the primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors.

In addition, the *DOT Cybersecurity Compendium*, section DOT-IA.2.b, requires information systems to use PIV cards assigned to DOT personnel as the system's primary authentication mechanism at both the system and application level.

Although DOT employees and contractors with network accounts are required to authenticate to the DOT network using a PIV card, unless an exemption has been granted and approved, we found that the Department has not transitioned all its information systems (e.g., major applications and general support systems) to use multifactor user identity authentication.

Specifically, we noted the following information security weaknesses related to PIV authentication:

- The Department has not transitioned 68 systems to be enabled to use PIV (or another form of two-factor authentication or an authentication mechanism was unspecified) at the application level or through inheritance from PIV access enforcement at the network level.
- 29 systems were PIV enabled; however, PIV was not enforced as the primary authentication method.
- 40 of 211 systems that contain Personally Identifiable Information (PII) were either not enabled to use PIV or did not require PIV authentication.

The lack of PIV compliance is attributed to multiple reasons including dependencies on other tasks and on technology, migrating away from technologies not PIV/Multifactor Authentication compliant, underestimating the time to complete deployment, a lack of funding/allocation,

[33] OMB Memorandum M-11-11, *Continued Implementation Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors*.

resources, documentation, and approved exclusions. In addition, the Department has indicated that systems which have not transitioned to PIV (or another form of two-factor authentication) already inherit PIV authentication from access to workstations and servers prior to access to non-PIV information system; however, evidence was not provided to support this assertion.

Unresolved weaknesses in identity and access management, particularly pertaining to authentication mechanisms, make it difficult for DOT to ensure its information systems are adequately secured and protected and place the systems and the Department at risk for compromise. Specifically, the lack of mandatory PIV/multifactor authentication means information systems are more susceptible to attacks on user accounts.

Account Management

The DOT *Cybersecurity Compendium*, section PL-4, requires DOT component employees and contractors with access to DOT component information systems consent to either a DOT-wide Rules of Behavior or Component provided Rules of Behavior, which is no less stringent. In addition, NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-2 Account Management, indicates that organizations should require approvals for requests to create information system accounts, and review accounts for compliance with account management requirements.

We also noted the following weaknesses related to account management controls:

- For 3 of 25 sampled DOT new hires with COE application accounts during the audit period, we were not provided with evidence of account creation or account approval, and access requests were incomplete.
- For 10 of 25 sampled DOT new hires with OST CSAM application accounts during the audit period, we were either not provided evidence of account creation or account approvals, access requests were incomplete, or user access requests were approved after CSAM user accounts were setup.
- In addition, for 15 of 25 sampled DOT new hires with COE application accounts, 1 of 25 new hires with CSAM accounts and 5 of 25 FAA new hires, we were not provided with evidence of a completed Rules of Behavior.
- Evidence of FAA's annual review for privileged user accounts and permissions for one system was not provided.

OCIO did not enforce the retention or completion of documentation for 1) granting system access based on user access approvals and completion of Rules of Behavior, and 2) did not ensure a review of privileged user accounts was performed. Control weaknesses in identity and access management may expose DOT to increased risk of data compromise and may lead to unauthorized access to DOT's information systems.

Background Investigation

DOT 1630.2C*, Personnel Security Management*, requires that all periodic background reinvestigations be initiated for all Moderate and High-risk positions as well as National Security positions within five years of the previous investigation. However, we noted that DOT did not consistently ensure employees had timely background reinvestigations conducted. Specifically, we noted the following issues:

- FAA had not conducted Moderate Risk reinvestigations for 1,261 individuals requiring reinvestigation since July 1, 2020. Based upon the *Moderate Risk Reinvestigation Project Plan*, FAA is tracking approximately 15,585 individuals requiring Moderate Risk reinvestigations.
- Based upon review of FAA personnel who were due for background reinvestigations, we determined reinvestigations were not initiated for 18 of 25 individuals sampled. Also, for 3 of the 25 individuals sampled, their reinvestigation was initiated after the previous investigation had expired, thus not initiated in a timely manner.
- Based upon a comparison of DOT personnel who required background reinvestigations to a listing of all personnel who had an investigation initiated/completed since the beginning of the audit period, we identified 1 of 18 individuals who did not have their reinvestigation initiated. This individual was employed in a position designated as "critical sensitive."

FAA indicated that they do not have the resources to complete the past due cases at one time and therefore have implemented a phased multi-year plan for completion. Within this plan entitled *FAA's Moderate Risk Reinvestigation Project Plan*, the Office of Personnel Security (AXP) is currently in phase 4 (as of May 26, 2021) to bring all past due Moderate Risk investigations up to date. In addition, because of the COVID-19 pandemic, FAA's plan for FY 2021 was modified to reflect their frequent inability to obtain fingerprints from their employees and contractors at more than 1,100 facilities across the United States and its territories.

FAA has also indicated that although they strive to submit reinvestigations to the Defense Counterintelligence and Security Agency (DCSA) prior to the five-year reinvestigation due date, several factors may create delays, including budget and availability of subjects due to training and leave, delays by the employee to complete and submit the electronic questionnaires for investigations processing (e-QIP) form in a timely manner, and personnel security workloads as initial investigations take priority over employee reinvestigations.

Without conducting reinvestigations in a timely manner, DOT is at risk of allowing individuals to access sensitive data and systems without a sufficient degree of investigation.

Metric Domain – Data Protection and Privacy

FISMA requires the Federal government to establish a privacy program and corresponding policies and procedures for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Documentation to be maintained as part of an effective privacy program includes PIAs, PTAs, and System of Records Notices (SORN). In addition, agencies are required to develop a data breach response plan for reporting, investigating, and managing a privacy-related breach.

DOT Business Owners should be collaborating with System Owners to ensure all privacy regulatory compliance reporting changes are entered and updated as required in the CSAM system and/or any other DOT tracking system in accordance with DOT Order 1351.18, *Departmental Privacy Risk Management Policy*. In addition, FAA requires that PTAs for its systems must be submitted to the FAA National Information Security and Privacy (IS&P) Security Assessment Branch at least 90 days prior to issuance of the ATO. Also, since PTAs expire, FAA requires that PTAs must be reviewed annually in accordance with FAA Order 1370.21, *FAA Information Security and Privacy Program Policy*. Additionally, DOT policy requires an annual privacy risk assessment be conducted as stated in the Privacy Implementation Memo (PIM) for Privacy Continuous Monitoring (PCM) memo issued October 16, 2019. The memo was issued in response to OMB Circular A-130, *Managing Information as a Strategic Resource*, which requires Federal agencies to establish a PCM strategy that supports the periodic verification and validation of privacy risk and mitigation strategies of information resources, including IT systems. The risk assessment is documented in either a PTA or PCM as appropriate prior to issuance of system authorization.

We noted that privacy risk management artifacts for 33[34] out of 63 sampled systems or 52 percent of DOT systems were either not current or not developed. These weaknesses were comprised of 19 FAA systems with a PTA that was not reviewed annually, 11 (FAA, FMCSA, FRA and PHMSA) systems that did not have a completed or current PTA prior to the issuance of their system authorization to operate, three systems (FAA and FHWA) did not have a PTA provided, and eight systems (FAA, FHWA, FRA, OST I&O COE, OIG,[35] and OST) with PII and classified with a PIA status of "required" under the E-Government Act but without a PIA. Also, 1 FRA system did not have the SORN requirement under the Privacy Act clearly determined.

Since OAs were not appropriately coordinating their privacy and cybersecurity risk management activities to ensure that all system authorization packages include appropriate privacy risk management plans, privacy documentation was not developed or maintained in a timely manner. The majority of the Department's privacy risk derives 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.

Metric Domain – Security Training

FISMA requires all Federal government personnel and contractors to complete annual security awareness training that provides instructions on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot ensure that personnel would have the knowledge required to ensure the security of the information systems and data.

We determined that DOT did meet its annual compliance threshold for security awareness and specialized training requirements by August 31, 2021. Departmental policy[36] requires OAs to ensure that by August 31, 2021, 95 percent of their personnel complete security awareness training for FY 2021. The Department came close to meeting this requirement. Overall, 94 percent of Departmental personnel have completed security awareness training. This was attributed to

[34] This number represents the # of unique systems with privacy weaknesses. Since some systems had more than one weakness, this number is not a sum of all the systems broken down subsequently.
[35] The PIA for OIG was within OST in the process of adjudication during the audit period.
[36] CAM 2021-001 - *DOT FY 2021 Implementation Guidance for Mandatory Security and Privacy Awareness Training*.

FAA and FMCSA not meeting the completion goal; however, they did attain at least an 87 percent completion rate. Additionally, the completion percentage for role-based training was 93 percent agency wide.

As ongoing and more frequent training reminders are not in place, there is a tendency for individuals to delay their completion of training. Meeting security training goals decreases the possibility that employees will engage in activities that could lead to security compromises. In addition, control weaknesses in the security training domain expose DOT to increased risk of unintentional and insecure user behavior in protecting the technology environment. Thus, DOT may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Recommendations:

We recommend that the DOT CIO take the following actions, in addition to addressing the prior open recommendations[37] related to the weaknesses noted for the Protect function:

3. Work with the FAA CIO and FMCSA Information Security System Manager (ISSM), to investigate and remediate cross-site scripting vulnerabilities identified in public facing web applications.
4. Work and coordinate with system owners to identify and remediate weak and default authentication mechanisms within their systems and the COE.
5. Develop and implement a process to facilitate centralized monitoring, oversight (by ISSMs and their alternates) and escalation efforts to ensure the timely completion of required security awareness training and role-based training for all DOT personnel leveraging an automated integrated solution(s) and dashboards.

[37] Prior FISMA open recommendations related to the findings noted within the "Protect" function: Recommendation 1 (DOT OIG Report Number FI-2014-006, 11/22/13), Recommendations 8 and 15 (DOT OIG Report #FI-2015-009, 11/14/2014), Recommendation 1 (DOT OIG Report #FI-2016-001, 11/05/15), Recommendations 6, 7, and 8 (DOT OIG Report # FI-2018-017, 1/24/2018); Recommendation 6 and 12 (DOT OIG Report Number FI-2019-023, 3/20/2019) and Recommendation 7 (DOT OIG Report Number QC2020002, 10/23/2019), Recommendations 2, 3, 4, 5, 6, 7, 8, 11, 12, 13, and 14 (DOT OIG Report Number QC2021003,10/26/2020). These recommendations are not being repeated within this report. Refer to Appendix C for details on these recommendations.

Security Function: Detect

Overview

Although DOT continues to enhance its implementation of various tools and processes to detect threats and vulnerabilities to improve its continuous monitoring program, much work remains to adequately measure and evaluate this progress and its effectiveness. As a result, DOT's Detect controls remain at the Defined level of maturity due to the inconsistent application of controls throughout the Department.

Metric Domain – Information Security Continuous Monitoring

The goal of Information Security Continuous Monitoring (ISCM) is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness. In addition, specific requirements as defined within DOT policies require system owners to develop a strategy for continuous monitoring of the information system to include assessing all security controls, including common and hybrid controls, implemented at the system level to be assessed on an annual frequency.[38]

The following weaknesses were identified related to ISCM:

- For 9 of 63 sample systems, or 14.3 percent, SCAs were not performed annually, or were not provided. Based on our sample, we estimate 66 of 431 systems, or 15.2 percent, did not perform SCAs annually, or could not provide evidence a SCA was completed (FAA, FMCSA, and MARAD).
- For 6 of 63 sample systems or 10 percent, the ISCM Plan was not provided, and their respective SCAs were not performed annually or SCA was not provided (5 systems) or was not approved/signed (1 system). (FAA, FMCSA, MARAD, OST I&O COE).

These weaknesses were attributed to a combination of reasons including pandemic restrictions affecting system decommissioning processes; SA&A documentation permitted to lapse during system decommissioning; management oversight; third party assessors not required to include all SA&A documentation within DOT deliverables; and an incorrect reliance upon other documents such as relying upon security plans in lieu of a system characterization or risk assessment document. Due to improper continuous monitoring activity completion, stakeholders may not be made aware of system risk or activities.

Recommendations:

Prior FISMA recommendations[39] related to the weaknesses noted in the Detect function remain open and we are not making new recommendations.

[38] DOT *Security Authorization & Continuous Monitoring Performance Guide*, September 2019, version 4.2 and FAA *Security Authorization Handbook*, December 2020, version 1,Section 3.5.

[39] Prior FISMA open recommendations related to the findings noted within the "Detect" function: Recommendation 4 (DOT OIG Report Number QC2020002, 10/23/2019) and Recommendations 2 and 8 (DOT OIG Report Number FI-2016-001, 11/5/15). These recommendations are not being repeated within this report.

Security Function: Respond

Overview

DOT has improved controls over the consistent communication of threat activities to senior agency officials and controls related to incident response plan updates and development were also improved in order to adequately measure and evaluate the incident response program and its effectiveness.

Metric Domain – Incident Response
Information security incidents occur on a daily basis. Agencies must have comprehensive policies and planning in place to respond to these incidents and report them to the appropriate authorities. The United States Computer Emergency Readiness Team (US-CERT) is to receive reports of incidents on unclassified Federal Government systems, and OMB requires the reporting of incidents that involve sensitive data, such as PII, within strict timelines.

OCIO's *Cyber Security Incident Response Plan* requires that when an incident, such as a security breach or interruption of service occurs, the OA must report the incident to the FAA Security Operations Center (SOC). The SOC analyzes the incident, categorizes it, and reports it to US-CERT. DOT's policy also requires the SOC to have full network visibility over all DOT systems, including systems operating on behalf of OAs by contractors and other Government organizations. Although prior year weaknesses related to the development of incident response plans, have not been addressed, overall, the Department has established policies, procedures, and processes governing incident response are characteristic of a program at a Consistently Implemented level of maturity.

Recommendations:

Prior FISMA recommendations[40] related to the weaknesses noted in the Respond function remain open and we are not making new recommendations.

[40] Prior FISMA open recommendations related to the findings noted within the "Respond" function: Recommendations 11 and 12 (DOT OIG Report Number QC2020002, 10/23/2019). These recommendations are not being repeated within this report.

Security Function: Recover

Overview

DOT has, for the most part, defined policies and procedures for developing, updating, and testing its contingency plans; however, weaknesses remain affecting the effectiveness of controls to ensure the program is consistently implemented across the Department.

Metric Domain – Contingency Planning
FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if loss of a system's availability occurs. Consideration of risk to an Agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. NIST SP 800-34, Revision 1*, Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods." Additionally, the system owner must test the contingency plan for the information system on an annual basis, in accordance with the *DOT Cybersecurity Compendium Supplement to DOT Order 1351.37 v4.2*, May 2018, section DOT CP-4 "Contingency Plan Testing."

DOT has not consistently implemented contingency planning processes to reach a level of maturity as defined by FISMA metrics to be an effective overall program.[41] For the sampled systems, we found contingency plans were either not developed or were not reviewed, updated in a timely manner, tested annually, or a BIA was not developed.

We found that four OAs tested had not implemented DOT's contingency plans and testing requirements for at least one system. We also found systems not meeting OMB and FISMA requirements for contingency planning and testing. Specifically:

- For 6 of 63 sampled systems, or 9.5 percent, contingency plans were not provided for some systems or were not updated timely (FAA and MARAD). Based on our sample, we estimate 38 of 431 systems, or 8.8 percent,[42] have contingency plans that have not been developed or updated timely.
- Testing of contingency plans was not performed for 10 of 63 sampled systems, or 15.9 percent, in accordance with DOT requirements (FAA, MARAD, FHWA, and OST I&O COE). Based on our sample, we estimate 66 of 431 systems, or 15.3 percent,[43] did not perform contingency plan testing in accordance with DOT requirements.
- For 3 of 63 systems, or 4.8 percent, a BIA was not developed (FAA).

Ineffective contingency planning processes were attributed to the following: were not completed; or due to management oversight, plans were not updated or tested in a timely manner. Additionally, scheduled testing of systems was impeded due to the COVID-19 pandemic.

[41] A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.
[42] Our 8.8 percent estimate has a margin of error of +/- 6 percentage points at the 90 percent confidence level.
[43] Our 15.3 percent estimate has a margin of error of +/- 7.4 percentage points at the 90 percent confidence level.

Effective contingency planning, including a BIA, and comprehensive testing is crucial to ensure organizational systems and data are available and IT systems and applications are resilient against outages and disruptions. Failure to consistently document contingency plans increases the risk that DOT will be inadequately prepared for system or service disruptions and outages. In addition, failure to comprehensively test and exercise documented plans increases the risk that weaknesses or areas of improvement won't be identified effectively in preparation for real-world contingency events.

Recommendations:

Prior FISMA recommendations[44] related to the weaknesses noted in the Recover function remain open and we are not making new recommendations.

[44] Prior FISMA open recommendations related to the findings noted within the "Recover" function: Recommendation 3 (DOT OIG Report # FI-2012-007, 11/14/2011), Recommendation 14 (DOT OIG Report Number QC2020002, 10/23/2019) and Recommendation 18 (DOT OIG Report #QC2021003, 10/26/2020). These recommendations are not being repeated within this report.

Conclusion

DOT relies on hundreds of information systems to carry out its missions, including safe air traffic control operations, and handling billions of taxpayer dollars. DOT's cybersecurity program must protect these systems from malicious attacks and other compromises that may put citizen safety or taxpayer dollars at risk. While DOT continues to update its policies and procedures, and maintain a Defined level of maturity, we continue to find persistent deficiencies in the implementation of policies and processes, which are necessary for an effective information security program. The cause for these deficiencies can be attributed to an inconsistent enforcement of an agency-wide information security program across the enterprise and ineffective communication between the Department and the OAs, inadequate efforts towards the remediation of prior year audit recommendations, accompanied by the lack of adequate leadership and oversight given the current senior agency information security officer (Acting CISO) is not assigned information security duties as their official primary duty.

Therefore, DOT needs to improve its performance monitoring to ensure controls are implemented and operating as intended for all systems and at all OAs and communicate security deficiencies to the appropriate personnel, who must take responsibility for implementing corrective actions and ensuring those actions are consistently performed. These deficiencies place DOT's information systems at an increased risk of compromise and make them a target for malicious attackers.

We are also recommending that DOT undertake a strategic analysis of the IG FISMA Metrics and the weaknesses identified in the audit, to develop a multi-year strategy and approach to include objective milestones, and resource commitments by the Department and the CIO that addresses the corrective actions necessary to show steady, measurable improvements towards an effective information security program.

Agency Comments and CLA Response

We provided DOT with our draft report on August 20, 2021, and received DOT's response on September 20, 2021, which is included in its entirety as an appendix to this report. In its response, the Department described that the Agency's top priority continues to be attention to cybersecurity, that they continue with efforts to reduce risk, and have begun efforts to further address cybersecurity weaknesses and risks, while continuing to support telework and filling of key positions such as CISO and the Chief Privacy Officer (CPO).

DOT concurs with recommendations 1 through 5 as written and provided targeted completion dates for related actions.

DOT concurs with recommendation 1 as written. DOT states that it plans to implement this recommendation by November 30, 2022. Therefore, we consider recommendation 1 resolved but open pending completion of planned actions.

DOT concurs with recommendation 2 as written. DOT states that it plans to implement this recommendation by December 31, 2022. Therefore, we consider recommendation 2 resolved but open pending completion of planned actions.

DOT concurs with recommendation 3 as written. DOT states that it plans to implement this recommendation by August 31, 2022. Therefore, we consider recommendation 3 resolved but open pending completion of planned actions.

DOT concurs with recommendation 4 as written. DOT states that it plans to implement this recommendation by March 31, 2023. Therefore, we consider recommendation 4 resolved but open pending completion of planned actions.

DOT concurs with recommendation 5 as written. DOT states that it plans to implement this recommendation by September 30, 2022. Therefore, we consider recommendation 4 resolved but open pending completion of planned actions.

Actions Required

We consider recommendations 1 through 5 resolved but open pending completion of planned actions.

Appendix A: Background

DOT Overview

Established in 1966, DOT sets Federal transportation policy and works with State, local, and private-sector partners to promote a safe, secure, efficient, and interconnected national transportation system of roads, railways, pipelines, airways, and seaways. DOT's overall objective of creating a safer, simpler, and smarter transportation system is the guiding principle as the Department moves forward to achieve specific goals. DOT employs more than 54,000 people in the OST and through 10 OAs and Bureaus, each with its own management and organizational structure.[45]

An Agency's information security program is considered effective once it achieves a rating of Level 4, *Managed and Measurable*. For DOT, secure information helps protect both taxpayers' dollars and citizens' safety since many of its systems support transportation related operations, including air traffic control and pilot licensing. Others support inspection and oversight for highway safety and hazardous material transportation.

DOT's 11 OAs manage the Department's 447 IT systems.[46] The Department relies on these systems to carry out its missions, including safe air traffic control operations, qualified commercial drivers, and safe vehicles. DOT must also ensure the integrity of data in reports that account for billions of dollars used for major transportation projects, such as highway construction and high-speed rail development. DOT's cybersecurity program is critical to protect these systems from malicious attacks or other compromises that may inhibit its ability to carry out its functions and missions.

DOT's operations rely on 447 IT systems, 326 (73 percent) of which belong to the Federal Aviation Administration (FAA). These systems represent an annual investment of approximately $3.5 billion[47] – one of the largest IT investments among Federal civilian agencies.

FISMA Legislation

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires Federal agencies to develop, document, and implement an Agency-wide information security program to protect their information and IT systems, including those provided or managed by another Agency, contractor, or other source.

FISMA also provides a mechanism for improved oversight of Federal Agency information security programs. FISMA requires Agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) a security incident response capability is established, and (3) information security management processes are integrated with the Agency's strategic and

[45] https://www.transportation.gov/sites/dot.gov/files/2020-11/2020-DOT-Agency-Financial-Report-508compliant_113020.pdf
[46] DOT's population of systems includes 447 systems as of February 1, 2021. For the purposes of this audit and our sample system selection, we excluded all systems that have an operational status of "Implementation" as these systems are still in development. Additionally, we excluded all systems included in the population that had the "FISMA Reportable" field marked as false or had a response in the "Type" field other than "Major Application" or "General Support System." This resulted in a population of 431 systems.
[47] https://www.transportation.gov/cio

operational planning processes. All agencies must also report annually to OMB and to Congressional committees on the effectiveness of their information security program.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the Agency. As specified in FISMA, the Agency CIO or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires Agency IGs to assess the effectiveness of Agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the FIPS to establish Agency baseline security requirements.

FY 2021 IG FISMA Reporting Metrics

OMB and Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. Accordingly, the *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[48]

The FY 2021 metrics are based on a maturity model approach and align to the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 3**. The FY 2021 metrics include a new SCRM domain within the Identify function area; however, the SCRM domain was not considered in the Identify framework function rating.

Table 3: Aligning the Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metric Domains
Identify	Risk Management and Supply Chain Risk Management[49]
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

[48] https://www.cisa.gov/publication/fy21-fisma-documents
[49] This domain was not considered in the Identify framework function rating for FY2021.

The foundational levels of the maturity model focus on the development of sound, risk-based policies, and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

Table 4: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Appendix B: Scope and Methodology

Scope

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

GAGAS 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. OIG contracted with us to conduct the review of the DOT information security program and practices subject to OIG's oversight. Although the 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.

For this year's review, OMB required IGs to assess 66 metrics in five 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. As documented in Table 4 of Appendix A, the maturity levels range 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, including its performance in five function areas – Identify, Protect, Detect, Respond and Recover – for the 12-month period ending on June 30, 2021.

Our scope was to determine whether DOT implemented an effective information security program and practices for the 12-month period between July 1, 2020 and June 30, 2021, with a data collection cut-off date of June 30, 2021. The effectiveness of the information security program is defined as achieving a certain maturity level for each function area and domain based on the unique challenges of the organization.

For this audit, we reviewed select controls for a sample of 63 systems from a total population of 431 DOT FISMA reportable systems in operation.[50] The sampled systems are broken down by the following number of systems by OA: FAA (41), PHMSA (2), OST (6), FHWA (2), FMCSA (2), FRA (2), FTA (2), MARAD (2), NHTSA (2) and OIG (2). One system was substituted for FRA, since it was determined the system was retired. Refer to Appendix E for the specific systems selected for testing.

We performed an external penetration test covering FAA's Knowledge Services Network (KSN), Service Difficulty Reporting System (SDRS), and Federal Motor Carrier Safety Administration's (FMCSA) License & Insurance System (L&I) and an internal vulnerability assessment and penetration test of the Infrastructure and Operations (I&O) Common Operating Environment (COE).

[50] We selected a stratified random sample from DOT's population of 431 FISMA Reportable Major Applications/General Support Systems noted as being in operation to assess the Agency's compliance with FISMA.

In addition, the audit included an assessment of effectiveness for each of the nine FY 2021 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions. The audit also included a follow up on prior audit recommendations to determine if DOT made progress in implementing the recommended improvements concerning its information security program and practices.

Audit fieldwork was performed during the period of February 2021 through August 2021.

Methodology

To accomplish the audit objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to DOT's information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls. Testing procedures included penetration testing.
- Reviewed the status of recommendations in the prior year FISMA report, including supporting documentation to ascertain whether the actions taken addressed the noted weaknesses.

DOT's population of systems includes 447 systems as of February 1, 2021. For the purposes of our sample, we excluded all systems that have an operational status of "Implementation" as these systems are still in development. Additionally, we excluded all systems included in the population that had the "FISMA Reportable" field marked as false or had a response in the "Type" field other than "Major Application" or "General Support System." This resulted in a population of 431 systems. We selected a stratified simple random sample with a minimum of two systems per strata from DOT's population of 431 FISMA Reportable Major Applications/General Support Systems noted as being in operation to assess whether the Agency's information security management program and practices were effective in accordance with the GAGAS and the FISMA.

For sample selection purposes, we divided the 431 systems into 15 strata based on the OA to which the system belonged and the FIPS 199 risk categorization. The sample size was determined to address the following two requirements:

1. In order to ensure adequate coverage of the different OAs, each OA must have at least two systems selected.
2. The confidence level used will be 90 percent and the expected margin of error will be 10 percent.

To determine the sample size based on the above requirements, we performed extensive simulations assuming various scenarios of non-compliance rates and sample sizes and determining their effect on the resulting margin of error. The simulations carried out represented a random draw of a sample of a given size and a random subsample of non-compliant systems

in that sample. The non-compliance rate determined from each simulated sample was extrapolated to the overall population based on well-established survey sampling theory.[51] The simulations were repeated 100 times, and the average estimates were obtained in this manner. We chose a sample size of 63 systems, which we estimated would result, on average, about a 10 percent margin of error.

In addition, we assessed DOT's technical controls by performing a vulnerability assessment and penetration test of one OST I&O (formerly ITSS) system, and three DOT information systems: two FAA systems and one FMCSA system, as part of the FISMA audit. These tests included web facing applications and general support systems. The internal and external penetration tests were conducted to determine the effectiveness of controls that prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the internal and external penetration test were incorporated into our FISMA audit results.

To perform our audit of DOT's information security program and practices, we followed a work plan based on the following guidance:

- OMB and DHS, *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*.
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53A*,* Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment.*
- NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*
- OMB A-130, July 28, 2016, *Managing Information as a Strategic Resource.*
- Public Law 115-390 -115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the "Secure Technology Act."*

[51] Cochran WG (1977) *Sampling Techniques, 3rd Edition*. John Wiley and Sons.

Appendix C: Current Year Status of Prior FISMA Report Recommendations

The following is the status of open recommendations from prior FISMA reports. The current status of prior year FISMA open recommendations was determined through a review of the Department's overall status of prior recommendations and testing the effectiveness of DOT's information security program and practices covering the period July 1, 2020 through June 30, 2021.

In addition, three prior year recommendations were closed during the audit period. Thus, of 69 open recommendations from prior FISMA reports, 66 recommendations remain open as of June 30, 2021.

Prior Years' FISMA Recommendations that Were Closed

Fiscal Year 2013, OIG Report Number FI-2014-006 *FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats*	
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.

Fiscal Year 2019, OIG Report Number QC2020002 *FISMA 2019: DOT's Information Security Program and Practices*	
Number	**Recommendation**
9	Document and implement a process to ensure incident response procedures related to the timely notification, reporting, updating, and resolution of security incidents are followed in accordance with policy.
10	Review and update the OCIO Cyber Security Incident Response Plan, documenting evidence of review and revisions within a history log.

Prior Years' FISMA Recommendations that Remain Open

Note*: These remaining open recommendations do not represent and are not intended to represent all recommendations which were closed within the respective years or reports identified.*

Fiscal Year 2010, OIG Report Number FI-2011-022 *FISMA 2010: Timely Actions Needed to Improve DOT's Cybersecurity*	
Number	**Recommendation**
14	Identify and implement automated tools to better track contractors and training requirements.

Fiscal Year 2011, OIG Report Number FI-2012-007 *FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information System*	
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 2013, OIG Report Number FI-2014-006 *FISMA 2013: DOT Has Made Progress, But Its Systems Remain Vulnerable to Significant Security Threats*	
Number	**Recommendation**
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 2014, OIG Report Number FI-2015-009 *FISMA 2014: DOT Has Made Progress but Significant Weaknesses in Its Information Security Remain*	
Number	**Recommendation**
8	Work with the components to develop a plan to complete annual Security Awareness Training (SAT) training within plan milestones and improve tracking. 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.

Fiscal Year 2015, OIG Report Number FI-2016-001 *FISMA 2015: DOT has Major Success in PIV Implementation, But Problems Persist In Other Cybersecurity Areas*	
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 CIO 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 2016, OIG Report Number FI-2017-008 *FISMA 2016: DOT Continues to make progress, but the Department's information security posture is still not effective*	
Number	**Recommendation**
1	Work with all OAs to complete expired authorizations and reinforce or strengthen policy requiring systems be reauthorized prior to their expiration dates.
2	Work with all OAs to perform a thorough CSAM quality review to ensure system documentation matches what is entered into CSAM. At a minimum, the review should verify that: (1) system authorization dates in CSAM match what is approved by the authorizing official; (2) POAMs are created and reported once a security weakness is found; and (3) authorizing officials are provided accurate documentation on all risks accepted.
3	Work with FAA, FHWA, FMCSA, FTA, MARAD, NHTSA, and OST to develop risk acceptance memos for the expired systems identified in this report.
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.

Fiscal Year 2016, OIG Report Number FI-2017-008 *FISMA 2016: DOT Continues to make progress, but the Department's information security posture is still not effective*	
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 2017, OIG Report Number FI-2018-017 *FISMA 2017: DOT's Information Security Posture is Still Not Effective*	
Number	**Recommendation**
3	For the COE and FAA, update procedures and practices for monitoring and authorizing common security controls to (a) require supporting documentation for controls continual assessments, (b) complete reauthorization assessments for the controls, (c) finalize guidance for customers' use of controls, and (d) establish communication protocols between authorizing officials and common control providers regarding control status and risks.
4	Verify that FAA's criteria regarding designation and definition of contractor systems conforms to DOT guidance, and that systems are correctly classified.
5	Implement controls to continuously monitor and work with components to ensure network administrators are informed and action is taken to disable system accounts when users no longer require access or have been inactive beyond established thresholds.
6	Complete PIV enablement and requirements for remaining information systems, except those that are subject to exclusions that are documented and approved.
7	Take action to fully implement mandatory use of PIV cards for VDI access.
8	Implement processes verifying that personnel performing certain security related roles receive specialized training needed to meet OCIO guidance.

Fiscal Year 2018, OIG Report Number FI-2019-023 *FISMA 2018: DOT's Information Security Program and Practices*	
Number	**Recommendation**
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.

Fiscal Year 2018, OIG Report Number FI-2019-023 *FISMA 2018: DOT's Information Security Program and Practices*	
Number	**Recommendation**
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.

Fiscal Year 2019, OIG Report Number QC2020002 *FISMA 2019: DOT's Information Security Program and Practices*	
Number	**Recommendation**
1	Perform a review of all POA&M items closed during the audit period to include supporting documentation and re-approve their closure.
2	Revise current security weakness management policies and procedures (documenting within a revision history table) to require documented evidence such as calendar appointments, meeting minutes, etc. in support of POA&M closure decisions to be uploaded into CSAM.
3	Work with the OA CIOs to review current assessment and authorization processes and implement a validation process to ensure updated security plans, ATOs and risk assessments are reviewed and updated to reflect all system (including privacy) controls, vulnerabilities, and that current risks are clearly presented to the authorizing officials
4	Work with the OA CIOs to develop mechanisms to ensure updated system security plans and assessments of security controls (that were previously assessed as not satisfied or partially satisfied) reflect current operational environments, including an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.

Fiscal Year 2019, OIG Report Number QC2020002 *FISMA 2019: DOT's Information Security Program and Practices*	
Number	**Recommendation**
5	Document OA subnets and OA responsibilities for devices and systems operating on the Common Operating Environment.
6	Document and implement network segmentation to reduce the attack surface or susceptibility of vulnerable and sensitive OA assets in the Common Operating Environment.
7	Work with OAs to remediate outstanding identity and access management weaknesses through implementation and closure of POA&Ms and control assessments to determine whether these risks were addressed.
11	Resolve any inconsistencies with respect to Departmental policies and procedures, which prescribe conflicting directions on whether DOT components are required to provide, develop and update incident response plans, documenting evidence of review and revisions within a history log.
12	Implement a process to ensure incident response plans are developed for all OAs and updated on at least an annual basis.
14	Work with the OA CIOs to remediate identified weaknesses in contingency plans and BIAs, such as missing information, lack of timely review, and inadequate approvals, demonstrated by updated contingency plans and BIAs.

Fiscal Year 2020, OIG Report Number QC2021003 *FISMA 2020: DOT's Information Security Program and Practices*	
Number	**Recommendation**
1	Require OST to either start utilizing the CSAM tool for its security control assessments or develop its own risk assessment policies and procedures as required by DOT's Cybersecurity Compendium.
2	Work with OAs to update privacy risk management procedures to ensure the completion, tracking, review, and approval of privacy plans and compliance documentation prior to system authorization or reauthorization. Components should engage the Departmental Chief Privacy Officer as appropriate.
3	Work with the Departmental Chief Privacy Officer to establish processes and procedures to notify Component Privacy Officers of systems scheduled for reauthorization so that required privacy risk management plans may be completed as required by policy.
4	Work with the Departmental Chief Privacy Officer to establish processes and procedures to determine Component compliance with Departmental policy requiring Privacy Risk Management plans be established prior to system authorization or reauthorization.
5	Coordinate with appropriate offices within the Office of the Secretary to develop and implement a strategy and solution(s) to ensure that supervisors, contracting officers, and contracting officer representatives enforce personnel onboarding and off boarding procedures, completion of the DOT Rules of Behavior and other IT requirements prior to being granted access to DOT networks, systems, and information, or have existing access revoked upon separation, in accordance with DOT policy.

Fiscal Year 2020, OIG Report Number QC2021003 *FISMA 2020: DOT's Information Security Program and Practices*	
Number	**Recommendation**
6	Strengthen its oversight of the configuration management processes performed by OAs to ensure configuration management plans are developed, kept up-to-date, and document requirements for each system.
7	Work with the FAA CIO to complete the revision of FAA Order 1800.66, Configuration Management Policy.
8	Work with OAs to implement oversight to address configuration change weaknesses and to ensure configuration changes to the information systems are properly documented and tracked through implementation and undergo a post-implementation review to verify procedures are followed.
9	Ensure that baseline configuration deviations are monitored, and deviations are approved to ensure that baseline compliance reports demonstrate a consistent and accurate application of baseline standards.
10	Consolidate to the enterprise Tenable Nessus system to ensure accessibility of baseline compliance and/or vulnerability assessment capabilities.
11	Ensure that missing security patches are either applied in accordance with DOT policy or that vulnerable software is otherwise remediated on the affected endpoints. In addition, ensure that missing security patches attributable to specific mission/business requirements are identified, control weaknesses are appropriately documented in POA&Ms, and that the authorizing official is aware of and has accepted risk for the associated weaknesses.
12	Document and implement a process to identify software end of life dates and require the development of implementation plans to eliminate unsupported software.
13	Work with FAA to secure a reliable funding stream for background reinvestigations.
14	DOT should devise strategies, consistent with Federal policies and guidance, to overcome the logistical challenges of fingerprinting during a pandemic or other events and circumstances which prevent the timely completion of background reinvestigations.
15	Work with the FAA CIO to review all systems listed in Appendix B of the FAA Air Traffic Operations (ATO) Information Security Continuous Monitoring (ISCM) Plan for NAS and Mission Support (MS) Systems to ensure the FAA ISCM plan is complete and accurate, making updates as needed.
16	Work with the OST IT Director to ensure an alternate processing site (including necessary agreements) is more clearly described within the contingency plan to permit the transfer and resumption of information system operations for essential missions/business functions consistent with recovery time objectives when the primary processing capabilities are unavailable, for those systems in accordance with the requirements of the Cybersecurity Compendium and NIST guidance.
17	Work with the PHMSA CIO to ensure an alternate storage site (including necessary agreements) is described within contingency plans to permit the transfer and resumption of information system operations for essential missions/business functions consistent with recovery time objectives when the

Fiscal Year 2020, OIG Report Number QC2021003 *FISMA 2020: DOT's Information Security Program and Practices*	
Number	**Recommendation**
	primary processing capabilities are unavailable, for those systems in accordance with the requirements of the Cybersecurity Compendium and NIST guidance.
18	Strengthen its oversight of the contingency planning processes performed by FMCSA, OST COE, OST Volpe, FAA, FRA, and MARAD to ensure contingency planning documentation is developed, updated, and tested in a timely manner, in accordance with policy.

Appendix D: Organizations Visited or Contacted

Office of the Secretary (OST)

Office of the Chief Information Officer (OCIO)

Federal Aviation Administration (FAA)

Federal Highway Administration (FHWA)

Federal Motor Carrier Safety Administration (FMCSA)

Federal Railroad Administration (FRA)

Federal Transit Administration (FTA)

Maritime Administration (MARAD)

National Highway Traffic Safety Administration (NHTSA)

Office of Inspector General (OIG)

Pipeline and Hazardous Materials Safety Administration (PHMSA)

Appendix E: Representative Subset of Sampled Systems

FAA

	System Name	Impact Level	Contractor System
1	Air Route Surveillance Radar Model 4	High	No
2	Airport Surface Detection Equipment - Model X	High	No
3	Office of Information and Technology Enterprise Data Centers	High	Yes
4	Cybersecurity Test Facility	High	No
5	Business Continuity Support System	High	Yes
6	Air Route Surveillance Radar Model 3 Common Air Route Surveillance Radar (CARSR)[52]	Moderate	No
7	Airport Cable Loop System	Moderate	Yes
8	Interim Voice Switch Replacement System	Moderate	Yes
9	Logistics and Inventory System	Moderate	Yes
10	Logistics Center Support System	Moderate	Yes
11	Remote Monitoring and Logging System	Moderate	No
12	Time Based Flow Management	Moderate	No
13	Web Configuration Management	Moderate	Yes
14	Aviation Safety Knowledge Management Environment - Enterprise Services	Moderate	No
15	Service Oriented Architecture-Infrastructure	Moderate	No
16	Risk Based Resource Targeting	Moderate	No
17	Investment Planning and Management	Moderate	No
18	AFN Infrastructure at Equinix DC-3/FCS Colo	Moderate	Yes
19	AIT Container Platforms	Moderate	Yes
20	Knowledge Services Network	Moderate	No
21	End User Devices	Moderate	Yes
22	Enterprise Information Management Platform	Moderate	No
23	FAA Cloud Services Amazon Web Services East/West	Moderate	No
24	FAA Cloud Services Colocation Services	Moderate	Yes
25	FAA Cloud Services Microsoft Azure Commercial	Moderate	Yes
26	Safety Issues Reporting System	Moderate	No
27	faa.gov Hosting Environment	Moderate	Yes
28	Service Difficulty Reporting System	Moderate	No
29	Simulator Inventory & Evaluation Scheduling System	Moderate	Yes
30	Computer Aided Engineering Graphics	Low	Yes
31	Enhanced Inventory Logistics and Maintenance System	Low	Yes
32	Environment and Occupational Safety and Health Training Needs Assessment Tool	Low	No
33	FAA Environmental Site Cleanup Report (ESCR) Automated Tracking System	Low	No
34	FAA Workplace Inspection Tool	Low	Yes

[52] The ARSR-3 system name was changed to CARSR in March 2021.

	System Name	Impact Level	Contractor System
35	Facility Power Panel System	Low	Yes
36	Flight Systems Laboratory Software Tool Set	Low	Yes
37	Sector Design Analysis Tool	Low	Yes
38	StarCaster	Low	Yes
39	System Wide Information Management Laboratory	Low	Yes
40	NextGen Prototyping Network	Low	No
41	Advanced Electronic Flight Strips	Low	No

OST

	System Name	Impact Level	Contractor System
1	Common Operating Environment	High	No
2	Cyber Security Assessment and Management	High	No
3	Consumer Complaints Application	Moderate	No
4	Aviation Decisions Data System	Moderate	No
5	Drug & Alcohol Testing Management Information System	Moderate	No
6	FedHR Navigator	Moderate	No

PHMSA

	System Name	Impact Level	Contractor System
1	PHMSA Data Mart	Moderate	No
2	Safety Monitoring and Reporting Tool	Moderate	No

FHWA

	System Name	Impact Level	Contractor System
1	National Tunnel Inventory	Moderate	No
2	Transportation Fellows Interns and Contractor System	Moderate	No

FMCSA

	System Name	Impact Level	Contractor System
1	Licensing & Insurance	Moderate	No
2	National Registry of Certified Medical Examiners System	Moderate	Yes

FRA

	System Name	Impact Level	Contractor System
1	Railroad Safety Information System	Moderate	No
2	FRA Hosting and Operational Support Technology Service	Moderate	Yes

FTA

	System Name	Impact Level	Contractor System
1	FTA General Support System	Moderate	No
2	Transit Integrated Appian Development Platform	Moderate	Yes

MARAD

	System Name	Impact Level	Contractor System
1	Electronic Invoice System	Moderate	No
2	Mariner Outreach System	Moderate	No

NHTSA

	System Name	Impact Level	Contractor System
1	NHTSA020: Artemis	Moderate	No
2	NHTSA301: Teleprocessing & Timesharing Services NDR Program	Moderate	No

OIG

	System Name	Impact Level	Contractor System
1	OIG Infrastructure	Moderate	No
2	JA-50 Lab	Moderate	No

Appendix F: Acronyms

AO	Authorizing Official
ATO	Authorization to Operate
ATO	Air Traffic Operations
AXP	Office of Personnel Security
CDM	Continuous Diagnostics Management
CCB	Change Control Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLA	CliftonLarsonAllen LLP
COE	Common Operating Environment
COVID	Coronavirus Disease
CSAM	Cybersecurity Assessment and Management System
DCSA	Defense Counterintelligence Security Agency
DOT	Department of Transportation
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GAGAS	Generally Accepted Government Auditing Standards
I&O	Infrastructure and Operations
IT	Information Technology
IS&P	Information Security and Privacy
ISCM	Information Security Continuous Monitoring
ITSS	Information Technology Shared Services
KSN	Knowledge Services Network
L&I	License and Insurance System
MARAD	Maritime Administration
MS	Mission Support
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
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plans of Actions and Milestones
PTA	Privacy Threshold Assessment
RMF	Risk Management Framework
SAR	Security Assessment Report
SAT	Security Awareness Training
SCA	Security Control Assessment
SCD	System Characterization Document
SCRM	Supply Chain Risk Management
SDRS	Service Difficulty Reporting System
SOC	Security Operations Center
SORN	System of Records Notices
SSP	System Security Plans
TCCB	Technical Configuration Control Board
US-CERT	United States Computer Emergency Readiness Team
VDI	Virtual Desktop Infrastructure
VOLPE	John A Volpe National Transportation Systems Center

Appendix G: Management Comments

U.S. Department of Transportation
Office of the Secretary

1200 New Jersey Avenue, SE Washington, DC 20590

Subject: **ACTION**: Management Response to OIG Draft Report - Federal Information Security Modernization Act (FISMA) for Fiscal Year 2021

From: Andrew R. Orndorff
Associate Chief Information Officer / Strategic Portfolio Management and Acting Chief Information Security Officer
Office of the Chief Information Officer

ANDREW R ORNDORFF Digitally signed by ANDREW R ORNDORFF Date: 2021.09.20 16:23:54 -04'00'

To: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

With the issuance of Executive Order (EO) 14028 - *Improving the Nation's Cybersecurity,* and the Department of Transportation's (DOT) response to multiple government-wide incidents and directives this past year, agency attention on Cybersecurity continues to be a top priority for DOT. The Department continued its commodity information technology (IT) transformation and shared service initiatives to achieve efficiencies and reduce risk, while maintaining an overall rating of "Managing Risk" from the Department of Homeland Security (DHS) for Fiscal Year 2021 under the EO 13800 risk management assessment methodology. The Department also began new efforts and made investments into enterprise capabilities to further address cybersecurity weaknesses and risks, while continuing to support maximum telework in response to COVID-19 and facing vacancies in key positions including the Chief Information Security Officer (CISO), and Chief Privacy Officer (CPO). These efforts and enhancements included:

- Achievement of 100 percent compliance with DHS Trustworthy E-mail requirements;
- Acquisition and deployment of endpoint detection and response (EDR) capabilities to improve monitoring, detection, and mitigation on DOT endpoints as part of DOT's zero trust solution architecture;
- Acquisition and implementation of cloud-based enterprise logging capabilities to better support DOT cyber incident detection and response capabilities; and
- Further enhancements to and automation of tracking and reporting on annual security awareness training performance to improve data quality, timeliness of reporting, and compliance with DOT requirements.

1

Upon review of the OIG draft report, we concur with all recommendations as written and will complete related actions as noted below:

Recommendation	Target Completion Date
1	November 30, 2022
2	December 31, 2022
3	August 31, 2022
4	March 31, 2023
5	September 30, 2022

We appreciate the opportunity to comment on OIG's draft report. If you have any questions, please contact Andrew R. Orndorff, Associate CIO/SPM and Acting CISO, at 202-366- 7111.

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety Hotline

https://www.oig.dot.gov/hotline
hotline@oig.dot.gov
(800) 424-9071

OUR MISSION

OIG enhances DOT's programs and operations by conducting objective investigations and audits on behalf of the American public.

1200 New Jersey Ave SE
Washington, DC 20590
www.oig.dot.gov