OST

Report QC2024042
September 30, 2024

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

U.S. Department of Transportation
Office of Inspector General

Highlights

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 | QC2024042 | September 30, 2024

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 Sikich 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

Our QCR disclosed no instances in which Sikich did not comply, in all material respects, with generally accepted Government auditing standards.

Our Recommendations

DOT concurs with all 10 of Sikich's recommendations. Sikich considers 10 recommendations resolved but open pending completion of planned actions.

Contents

U.S. Department of Transportation
Office of Inspector General

Memorandum

Date: September 30, 2024

Subject: INFORMATION: Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices | Report No. QC2024042

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 (OMB). To meet this requirement for fiscal year 2024, we contracted with Sikich, an independent public accounting firm, to conduct this audit subject to our oversight.

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

Sikich found that DOT's information security program is at the Defined maturity level—the second lowest of five levels in the maturity model for information security programs. To be considered effective, an agency's program must be at level 4, Managed and Measurable. Consequently, DOT's program is not effective. Sikich made the following recommendations to DOT's Chief Information Officer to help the Department develop a more mature and effective information security program.

1. Work with the Cyber Security Assessment and Management (CSAM) system owner to resolve the technical issues to ensure the CSAM Plan of Action and Milestones (POA&M) reporting function is accurate and conduct oversight of the Operating Administrations to ensure that the POA&M entries meet the requirements of Information Technology (IT) Implementation Memorandum 2023-010A, *DOT Supplemental Requirements for IT Security POA&M Management*.

2. Strengthen procedures for maintaining a comprehensive and accurate cloud system inventory, which includes reconciling CSAM data to the listing of cloud service providers submitted by the Operating Administrations.

3. Enforce password polices to ensure passwords are harder to guess and extend the timeframe in which individuals can enter the next password. Further, use cryptographically protected channels to transmit passwords.

4. Document and implement procedures to review on a periodic basis users with administrative rights and privileged groups with access to domain controllers.

5. Implement protections to restrict access to system tools used to create and manage shadow copies of the hard drive.

6. Document and implement procedures to analyze user account passwords against lists of commonly used and compromised passwords and require users to reset weak or compromised passwords.

7. Direct the DOT Information Assurance and Privacy Management Office and Breach Assessment and Response Team to implement annual testing of the Breach Notification Controls, as required by DOT Order 1351.19, *Personally Identifiable Information Breach Notification Controls*.

8. Complete the DOT workforce assessment, which includes the entire DOT IT and cybersecurity workforce.

9. Update the Office of Chief Information Officer *Cybersecurity Incident Response Plan* to incorporate lessons learned from the security incident and ensure that it reviews and updates the plan annually.

10. Document and implement a plan to issue policy, implementation instructions, procedures, and configuration guidance to support Departmental enterprise event logging in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*.

We performed a quality control review (QCR) of Sikich's report, dated September 20, 2024 (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. Sikich is responsible for its independent auditor's report and the conclusions expressed in that report. Our QCR disclosed no instances in which Sikich 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 contact me.

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

Agency Comments and OIG Response

On August 8, 2024, Sikich provided DOT with its draft report and received DOT's response on August 28, 2024. DOT's response is included in its entirety as part of the attached independent auditor's report. DOT concurred with all 10 of Sikich's recommendations and provided appropriate planned actions and estimated completion dates.

Actions Required

We consider all 10 recommendations resolved but open pending completion of planned actions.

Exhibit. List of Acronyms

CSAM	Cyber Security Assessment and Management
DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act
IT	Information Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
QCR	quality control review

Attachment. Independent Auditor's Report

PERFORMANCE AUDIT OF THE UNITED STATES DEPARTMENT OF TRANSPORTATION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR 2024

SUBMITTED TO THE
DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

PERFORMANCE AUDIT REPORT

SEPTEMBER 20, 2024

ACCOUNTING TECHNOLOGY ADVISORY

SIKICH®

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

September 20, 2024

Inspector General
United States Department of Transportation

Sikich CPA LLC (Sikich)[1] is pleased to submit the attached report detailing the results of our performance audit of the U.S. Department of Transportation's (DOT's or the Department's) information security program, in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), for the 12 months ending on June 30, 2024. FISMA requires federal agencies, including DOT, to perform an annual independent evaluation of their information security programs. FISMA states that the evaluation is to be performed by the agency Inspector General (IG) or by an independent external auditor as determined by the IG. The DOT Office of Inspector General engaged Sikich to conduct this performance audit to assess the effectiveness of DOT's information security program and practices in accordance with Generally Accepted Government Auditing Standards and with FISMA.

The audit covered the period from July 1, 2023, through June 30, 2024. We performed audit fieldwork from November 2023 to July 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. These 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. We describe our objective, scope, and methodology further in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance provided by DOT management and staff.

Sikich CPA LLC

Alexandria, VA

[1] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's federal practice, including its work for the Department of Transportation Office of Inspector General.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (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 their agency's information security program and practices. The 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's (DOT's or the Department's) Office of Inspector General (OIG) engaged Sikich CPA LLC (Sikich)[2] to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of DOT's information security program and practices. The objective of this performance audit was to assess the effectiveness of DOT's information security program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with FISMA.

The OMB and the Department of Homeland Security (DHS) annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, the OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.[3] This memorandum describes the methodology for conducting FISMA audits and the process for federal agencies to report to OMB and, where applicable, DHS. According to that memorandum, each year IGs are required to complete IG FISMA Reporting Metrics[4] to independently assess their agency's information security program.

For this year's review, IGs were required to assess 20 core[5] and 17 supplemental[6] IG FISMA Reporting Metrics across five security function areas—Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency's information security program and the maturity level of each function area. The maturity levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*. To be considered effective, an agency's information security program must be rated at Level 4: *Managed and Measurable,* or above. See **Appendix A** for additional background information on the FISMA reporting requirements.

For this audit, we reviewed selected controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020), supporting the fiscal year (FY) 2024 IG FISMA reporting metrics, for a

[2] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's federal practice, including its work for DOT's OIG.
[3] See OMB M-24-04 at https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf
[4] See the Fiscal Year (FY) 2023 – 2024 IG FISMA Reporting Metrics at https://www.cisa.gov/sites/default/files/2023-02/Final%20FY%202023%20-%202024%20IG%20FISMA%20Reporting%20Metrics%20v1.1_0.pdf. We provided DOT's OIG with our responses to the FY 2024 IG FISMA Reporting Metrics as a separate deliverable under the contract for this audit.
[5] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.
[6] Supplemental metrics are assessed at least once every 2 years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

sample of DOT information systems. The audit covered the period from July 1, 2023, through June 30, 2024. We performed our audit fieldwork from November 2023 to July 2024.

II. SUMMARY OF RESULTS

DOT's overall effectiveness of its information security program and practices in accordance with FISMA did not meet the requirements to be considered effective. Specifically, DOT is at Level 2: *Defined*—the second-lowest level in the maturity model for an information security program and therefore not effective. We noted that four functional areas achieved a maturity level of Level 2: *Defined* and one functional area achieved a level of Level 3: *Consistently Implemented* for an overall maturity level of Defined for the security program. **Table 1** below summarizes the overall maturity levels for each security function and domain in the FY 2024 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions[7]	Maturity Level by Function	Domain	Maturity Level by Domain
Identify	Level 2: *Defined*	Risk Management	Level 2: *Defined* (Not Effective)
Identify	Level 2: *Defined*	Supply Chain Risk Management (SCRM)	Level 1: *Ad Hoc* (Not Effective)
Protect	Level 2: *Defined*	Configuration Management	Level 2: *Defined* (Not Effective)
Protect	Level 2: *Defined*	Identity and Access Management	Level 2: *Defined* (Not Effective)
Protect	Level 2: *Defined*	Data Protection and Privacy	Level 2: *Defined* (Not Effective)
Protect	Level 2: *Defined*	Security Training	Level 2: *Defined* (Not Effective)
Detect	Level 2: *Defined*	Information Security Continuous Monitoring (ISCM)	Level 2: *Defined* (Not Effective)
Respond	Level 3: *Consistently Implemented*	Incident Response	Level 3: *Consistently Implemented* (Not Effective)
Recover	Level 2: *Defined*	Contingency Planning	Level 2: *Defined* (Not Effective)
Overall	**Level 2: *Defined* (Not Effective)**		

Source: Sikich's assessment of DOT's information security program controls and practices based on the FY 2024 IG FISMA Reporting Metrics.

DOT has established several information security program controls and practices that are consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, DOT has:

- Continued implementing its Continuous Diagnostics and Mitigation (CDM) program to obtain additional tools and dashboards to monitor its security posture.

[7] 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.

- Established an integrated project team to address prior-year recommendations and engaged governance stakeholders to implement enhanced processes to improve the monitoring of information system compliance.

However, DOT continues to face significant challenges in the consistent implementation of its information security program and associated monitoring across the Department. These challenges have resulted in a static overall level of maturity in DOT's information security program, which can be attributed to multiple key factors, limitations, and dependencies, including—but not limited to—the following:

- DOT has published several updated information security program controls and practices, including a revised Compendium and security control catalog, as well as Information Technology Implementation Memorandums (ITIMs). However, these policies and directives still require additional cycle time for adoption across the Department and to demonstrate control effectiveness.
- Although DOT continues to increase its adoption of multifactor authentication (MFA) for its information systems, the recent requirement to include Operational Technology (OT)[8] systems in MFA implementation plans has impacted implementation targets. In addition, DOT experienced delays in compliance due to technology requirements.
- DOT continues to implement data loss prevention (DLP) controls to further prevent or restrict data loss. However, DOT has not yet completed the deployment of tools and functionality. Existing controls provide limited protections from data loss and transference of personally identifiable information (PII) and sensitive data.
- DOT engaged additional resources for the governance and management of activities to focus on improving its programs and policies. However, because these programs—such as adopting a zero-trust[9] architecture and performing prior-year weakness remediation efforts—are still in their initiation phase, they have not reached a sufficient level of maturity to make a significant impact on the Department's security posture.
- DOT's recent transition to the Department of Justice's Cyber Security Assessment and Management (CSAM)[10] system could provide opportunities for better workflow and standardization of security assessment and authorization (SA&A) of systems, as well as for improved reporting of DOT's FISMA-reportable systems.

In addition, DOT has outstanding prior-year recommendations that significantly impact its ability to improve its IG FISMA Reporting Metrics maturity levels. Specifically, at the beginning of the 2024 FISMA audit, DOT had 71 open recommendations from prior FISMA audits dating from 2011 through 2023. During our 2024 FISMA audit, we found that DOT took corrective actions to address 24 of the recommendations, and we consider those recommendations closed. Corrective actions are still needed to resolve the other 47 open recommendations.[11]

[8] NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy* (December 2018), defines Operational Technology (OT) systems as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). Examples include industrial controls systems and physical access control mechanisms.

[9] Executive Order 14028, *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021), requires Federal agencies to implement a zero-trust architecture, which is a security model of a set of system design principles and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries.

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

[11] See Appendix C for the status of prior-year recommendations.

Furthermore, some of these recurring security weaknesses that present a significant risk to DOT include unsupported software, missing patches, and configuration weaknesses. These weaknesses may allow unauthorized access into mission-critical systems and data. Many of these vulnerabilities have existed since they were first identified in the FY2019 FISMA audit. As a result, the assessment team was able to exploit certain vulnerabilities to obtain unauthorized elevated user permissions/privileges and access system resources.

DOT has longstanding security deficiencies similar in type and risk level to findings in prior years and, overall, has inconsistently implemented its security program. Consequently, we noted new and repeat weaknesses in all nine IG FISMA metric domains encompassing the Department's agency-wide program. Specifically, the audit identified continued deficiencies related to the Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning domains of the IG FISMA Reporting Metrics.

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),[12] new and emerging federal information security requirements, and DOT's limited progress in the remediation of prior-year audit recommendations. Further, DOT's efforts to modernize its technology and adjust to changes in personnel and new leadership, changes in management's direction for federal information security requirements (such as zero trust and MFA), and new information security programs and process improvements have impacted its ability to address deficiencies that impact multiple FISMA metric domains.

Additionally, to demonstrate measurable improvement in establishing an effective information security program, DOT must focus on remediating prior-year recommendations in a timely manner and prioritizing those recommendations that relate to the core metrics. Implementing more of these recommendations will help DOT to mature its information security program and bring it closer to effectiveness. In addition, as recommended in prior years, DOT should consider developing a long-term strategy that includes committing resources to address corrective actions as necessary to show steady, measurable improvement in its information security program. Developing such a strategy may require DOT to allocate sufficient resources, including staffing, to remediate audit recommendations in a timely manner.

DOT has taken a new approach to addressing cyber risk in terms of strategies and personnel. DOT is in the development phase of this approach. Once DOT has developed and finalized its zero-trust initiative strategy, this strategy should provide a more comprehensive approach to strengthening DOT's cybersecurity posture. However, these efforts could take several years to fully implement across the Department. These zero-trust efforts should enhance controls in the following FISMA metric domains: Risk Management, Configuration Management, Identity and Access Management, Information Security Continuous Monitoring, and Incident Response; however, they will not resolve all of DOT's deficiencies in meeting the FISMA requirements.

[12] DOT employs almost 55,000 people across the country, in the Office of the Secretary of Transportation (OST) and its operating administrations and bureaus, each with its own management and organizational structure. https://www.transportation.gov/administrations

At present, the weaknesses that we identified (as summarized in **Table 2**) leave DOT operations and assets at risk of unauthorized access, misuse, and disruption. Although the majority of these weaknesses were similar to weaknesses reported in prior years, with corresponding recommendations remaining open, we made 10 new recommendations to help the Department address challenges in developing a mature and effective information security program. Additionally, 47 prior-year recommendations remain open.[13]

Table 2: FY 2024 IG FISMA Metric Domains Mapped to Weaknesses Noted in 2024 DOT FISMA Audit

FY 2024 IG FISMA Metric Domains	Weaknesses Noted
Risk Management	DOT did not provide, maintain, or monitor SA&A documentation, plans of action and milestones (POA&Ms) did not meet DOT policy, and DOT does not maintain a complete and accurate inventory of its cloud-based systems and hardware assets.
Supply Chain Risk Management	Prior-year weaknesses remain open related to the development of a supply chain risk management strategy.
Configuration Management	Critical and high-risk security vulnerabilities continue related to patch management, configuration management, and unsupported software; noncompliance with configuration baselines; inadequate or missing configuration management plans; and DOT not consistently implementing change management procedures for high-risk sampled systems.
Identity and Access Management	DOT has not effectively managed and reviewed privileged user accounts, transitioned all its information systems (e.g., major applications and general support systems [GSS]) to use MFA, and consistently ensured that it conducts background investigations and reinvestigations.
Data Protection and Privacy	Implementation of data protection and privacy controls was not effective across DOT with regard to data exfiltration, encryption of sensitive data, and data breach response testing.
Information Security Continuous Monitoring	DOT did not properly complete, provide, or perform annual information security continuous monitoring (ISCM) of controls and assessment plans.
Security Training	DOT has not developed a current workforce assessment for privileged and non-privileged users, privileged users have not completed role-based training (RBT), and new users have not completed security awareness training (SAT).
Incident Response	DOT has not issued policies and procedures to support Departmental enterprise event logging (EL) requirements in accordance with OMB M-21-31[14] requirements and did not reach the EL1,[15] EL2,[16] and EL3[17] maturity levels by OMB's required due dates. Further, DOT did not update the Office of Chief Information Officer (OCIO) Cybersecurity Incident Response Plan on an annual basis and to include lessons learned from a recent incident.
Contingency Planning	For the sample of DOT systems, we noted weaknesses related to the development, maintenance, and testing of contingency plans, as well as the lack of documentation for business impact analyses (BIAs), identification of alternate storage or processing sites, and data backups.

Source: Sikich's assessment of DOT's information security program controls and practices based on the FY 2024 IG FISMA Reporting Metrics.

[13] See Appendix C for the status of prior-year recommendations.
[14] OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).
[15] Per OMB M-21-31, EL1 maturity level signifies only logging requirements of highest criticality are met.
[16] Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.
[17] Per OMB M-21-31, EL3 maturity level signifies logging requirements at all criticality levels are met.

The following section provides a detailed discussion of the audit results. **Appendix A** provides background information on FISMA. **Appendix B** describes the objective, scope, and methodology of the audit. **Appendix C** provides the current status of prior-year FISMA report recommendations. **Appendix D** provides the organizations we visited or contacted. **Appendix E** identifies the representative subset of sampled systems. **Appendix F** provides a listing of acronyms used throughout this report. **Appendix G** contains management comments to the report.

III. AUDIT RESULTS

The following section of the report describes the key controls underlying each function and domain and our assessment of DOT's implementation of those controls. We have organized our conclusions and ratings by function area and domain to help orient the reader to deficiencies as categorized by NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).

Security Function: Identify

The objective of the Identify function is to develop an organizational understanding of the business context and the resources that support functions that are critical for managing cybersecurity risk to systems, people, assets, data, and capabilities. We determined that the maturity level of DOT's Identify function is Level 2: *Defined*.

Risk Management

An agency with an effective risk management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk management program.

We determined that the maturity level of DOT's Risk Management domain is Level 2: *Defined*. DOT has advanced its risk management program by publishing a revision to the *DOT Cybersecurity Compendium* and organization-defined parameters in 2024 to describe its entity-wide information security risk management program and risk management framework.

However, we noted that DOT has 12 open prior-year recommendations in the Risk Management domain that relate to documenting and implementing an enterprise risk management program, ensuring adequate evidence of closure of security weaknesses, and requiring the authorizing official to review and approve system risks across the organization.[18]

In 2024, we identified risk management weaknesses in the creation, maintenance, monitoring, and retention of SA&A documentation; management of POA&Ms; and maintenance of a complete and accurate inventory of DOT information systems and hardware asset inventories.

The following sections detail the weaknesses we noted in DOT's risk management framework.

[18] See Appendix C for additional information regarding these prior-year recommendations.

Security Assessment and Authorization

Departmental policies[19] require OAs to annually assess security controls for their information systems and operating environments and examine the following security documentation: system security plans (SSP), risk assessments, and security categorization documents. However, we noted the following weaknesses related to SA&A processes:

- For 3 of 61 sampled systems, or 4.9 percent, the Authorization to Operate (ATO) was not current (Maritime Administration [MARAD] and Office of the Secretary [OST]).
- For 15 of 61 sampled systems, or 24.6 percent, OAs did not annually review the SSP or did not provide an SSP for review (Federal Aviation Administration [FAA], MARAD, and OST). Based on our sample, we estimate that OAs did not review an SSP annually or did not provide an SSP for review for 112 of 443[20] systems, or 25.3 percent.[21] [22]
- For 20 of 61 sampled systems, or 32.8 percent, OAs did not have a current risk assessment (as documented within a Security Assessment Report [SAR]); did not include risk categorization for likelihood, impact, and mitigation in the risk assessment; or did not provide a risk assessment (FAA, Federal Motor Carrier Safety Administration [FMCSA], MARAD and OST). Based on our sample, we estimate that OAs did not have a current risk assessment, did not include risk categorization in their risk assessments, or did not provide a risk assessment for review for 163 of 443 systems, or 36.7 percent.[23]
- For 16 of 61 sampled systems, or 26.2 percent, OAs did not provide the security categorization document or did not include the risk categorization for confidentiality, integrity, and availability in the SSP (FAA and OST). Based on our sample, we estimate that OAs did not provide security categorization documentation for review or did not include the risk categorization in the SSP for 133 of 443 systems, or 30 percent.[24]

SA&A deficiencies are attributed to a variety of causes, such as the inability of the Department and OAs to maintain complete and current documentation related to risk and security controls for FISMA-reportable systems in CSAM; inadequate continuous monitoring and updating of security measures or artifacts to remediate risks and vulnerabilities; OAs allowing some assessment and authorization documentation to expire due to the absence of an ATO package; and changes to the system's environment.

Without assessing system risks based on current, accurate, and complete SSPs on a continuous basis, DOT does not have reasonable assurance that it has reduced risk to an acceptable level and controls are operating effectively, and this may expose the Department to information loss, fraud, or abuse. In addition, the lack of adequate and/or timely security plans,

[19] DOT *Security Authorization & Continuous Monitoring Performance Guide,* version 4.2 (September 2019), and FAA *FY24 Security Authorization Handbook*, version 1 (October 2022).
[20] DOT's population of systems includes 458 FISMA-reportable systems as of November 6, 2023. For the purpose of this audit and our sample system selection, we 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 443 systems.
[21] Our 25.3 percent estimate has a margin of error of +/- 9.5 percentage points at the 90 percent confidence level.
[22] We performed an extrapolation of selected results to the population of 443 systems. These extrapolated estimated error rates took into consideration the stratification of the system sampled to derive the weighted point estimate of the error rate, with a 90 percent confidence level. Consequently, the weighted error rates are not equal to the ratio of errors observed during the audit divided by 61, the system sample size. Please refer to Appendix B: Objective, Scope, and Methodology of this report, which further describes the system selection methodology.
[23] Our 36.7 percent estimate has a margin of error of +/- 11 percentage points at the 90 percent confidence level.
[24] Our 30.0 percent estimate has a margin of error of +/- 10 percentage points at the 90 percent confidence level.

assessments, and/or continuous monitoring limits the ability of authorizing officials to make effective decisions regarding the risk of compromise created by system operations.

Plans of Action and Milestones

The DOT *ITIM 2023-10A DOT Supplemental Requirements for Information Technology (IT) Security POA&M Management* (September 28, 2023) outlines management and reporting requirements for agency POA&Ms, including documentation requirements for the deficiency, remediation actions, responsible parties, and approvals. The establishment, tracking, and remediation of information security weaknesses through the POA&M process is a significant process in the NIST risk management framework.

However, we noted that DOT did not effectively manage POA&Ms throughout the Department. According to DOT's central reporting database, CSAM, the Department had approximately 11,358 open POA&Ms as of June 30, 2024, compared to 10,862[25] open POA&Ms in 2023. Of the total number of open POA&Ms, 10,272—or 90 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, based upon examination of 10 DOT OAs' POA&Ms created since October 1, 2023, we noted the following:

- All 10 of the OAs did not consistently populate the "POA&M Source (work activity that initiated POA&M)" field (FAA, Federal Highway Administration [FHWA], FMCSA, Federal Railroad Administration [FRA], Federal Transit Administration [FTA], MARAD, National Highway Traffic Safety Administration [NHTSA], OIG, OST, and Pipeline and Hazard Materials Safety Administration [PHMSA]).
- Two of the ten OAs did not consistently map the POA&Ms to cybersecurity controls (FMCSA and OIG).
- One of the ten OAs did not consistently document the estimated cost for remediation (FRA).
- One of the ten OAs had not yet determined the "POA&M Planned Start Date" and "POA&M Planned Finish Date" and had not documented POA&M milestones in sufficient granularity to track remediation progress. In addition, we found that the OA had surpassed the POA&M Planned Start Date without setting a new Planned Start Date or Actual Start Date (MARAD).

DOT OCIO management indicated that these inconsistencies are primarily due to clerical errors. To address this issue, DOT plans to implement remediation measures that include providing weekly CSAM training and establishing standard operating procedures to ensure consistent documentation of POA&Ms. Management from the FTA and NHTSA OAs stated that the discrepancies occurred due to a CSAM update implemented mid-April 2024. The rollout of new work source selections for the "POA&M Source (work activity that initiated POA&M)" field in CSAM had inadvertently set previous selections to a blank status. FHWA management indicated that when creating a POA&M, CSAM did not identify the "POA&M Source (work activity that initiated POA&M)" field as required, as denoted with asterisks. OIG management indicated the CSAM does not have technical controls to enforce completion of the "POA&M Source (work activity that initiated POA&M)" field or to require personnel to map the POA&M to cybersecurity controls.

[25] *Quality Control Review on the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices* (DOT OIG Report Number QC2023047, September 27, 2023).

Without properly managing POA&Ms, DOT is at risk of inadequately tracking or remediating operating systems and applications with known security weaknesses. Furthermore, without adequate plans for known security weaknesses, DOT cannot ensure that it will fully mitigate corresponding security risks.

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.[26] However, DOT has not maintained a complete and accurate inventory of its information systems (including cloud systems/platforms). Specifically, DOT's cloud system inventory did not consistently align with the department-wide system inventory listing within CSAM, and DOT did not provide a comprehensive hardware inventory listing, as discussed below.

Cloud System Inventory

Although DOT's cloud system inventory as of March 29, 2024, matches the inventory counts of cloud systems within the OCIO FY 2024 Quarter 1 FISMA Metrics (dated January 29, 2024), DOT's cloud system inventory listing does not consistently align with the cloud system inventory listing within CSAM (report generated on February 22, 2024). Specifically, we noted the following exceptions:

- DOT's cloud system inventory contained 11 cloud systems that were not included in the CSAM inventory.
- The CSAM inventory contained five cloud systems that were not included in the Department's cloud inventory.

DOT management indicated that it updates the comprehensive cloud inventory manually. This update process is based on the quarterly IT Spend Plan,[27] where OAs add their existing cloud service providers. The inventory reported for OCIO FISMA Metrics may not accurately reflect the inventory recorded in CSAM.

Given DOT's reliance on manual processes to update its cloud inventory, there is an increased risk of error. If DOT is not aware of all IT assets residing in its environment, it may not appropriately manage and protect these assets. The absence of an accurate cloud inventory creates a risk that the Department may not accurately assess and allocate security resources, potentially leaving some assets vulnerable.

Hardware Inventory

NIST standards[28] 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.

[26] DOT's *FISMA Inventory Guide*, Version 1.1 (September 2013).
[27] OA IT Spend Plans are required per *DOT Order 1351.39 Information Technology Management Policy* and the *FY23 Spring Update IT Spend Plan Memo Guidance*.
[28] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations* (September 2020), security control CM-8, Information System Component Inventory.

DOT has not provided a comprehensive inventory of hardware assets connected to the network in support of the hardware inventory counts reported in the CIO FISMA Metrics. DOT attributed this lack of comprehensive hardware assets to the recent deployment of CDM tools to improve inventory accuracy and completeness.

The lack of a formalized process to reconcile hardware asset inventories received from the OAs with the Department's hardware asset inventory counts has resulted in ongoing discrepancies, thus undermining the integrity and accuracy of the inventory process.

Supply Chain Risk Management

An agency with an effective SCRM program (1) ensures that external providers' products, system components, systems, and services are consistent with the agency's cybersecurity and SCRM requirements, and (2) reports qualitative and quantitative performance measures on the effectiveness of its SCRM program.

We determined that the maturity level of DOT's SCRM domain is Level 1*: Ad Hoc*. We noted that DOT has one open prior-year recommendation from a previous FISMA report related to the development of a comprehensive SCRM strategy and an implementation plan to guide and govern supply chain risk.[29] Specifically, DOT's *Cybersecurity Implementing Instructions: Cyber Supply Chain Risk Management* and *IT Enterprise Risk Management ITIM* remained in draft form.

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. Work with the CSAM system owner to resolve the technical issues to ensure the CSAM POA&M reporting function is accurate and conduct oversight of the OAs to ensure that the POA&M entries meet the requirements of ITIM 2023-010A, *DOT Supplemental Requirements for IT Security POA&M Management*.

2. Strengthen procedures for maintaining a comprehensive and accurate cloud system inventory, which includes reconciling CSAM data to the listing of cloud service providers submitted by the OAs.

[29] See Appendix C for additional information regarding these prior-year recommendations.
[30] Prior FISMA open recommendations related to the findings noted within the "Identify" function: Recommendations 3, 4, and 7 (DOT OIG Report # FI2017008, November 9, 2016); Recommendations 4, 9, and 11 (DOT OIG Report Number FI2019023, March 20, 2019); Recommendations 1 through 4 (DOT OIG Report Number QC2020002, October 23, 2019), Recommendations 1 and 2 (DOT OIG Report Number QC2022006, October 25, 2021) and Recommendation 1 (DOT OIG Report Number QC2022042, September 28, 2022). We are not repeating these recommendations within this report. Refer to Appendix C for details on these recommendations.

Security Function: Protect

The objective of the Protect function is to develop and implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event. DOT's Protect controls, which cover configuration management, identity and access management, data protection and privacy, and security training, were not effective and were not consistently implemented across the Department. In 2024, weaknesses in DOT's IT environment continued to contribute to deficiencies in system configuration, data protection and privacy, and access controls. We determined that the maturity level of DOT's Protect function is Level 2: *Defined*.

Configuration Management

An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.

We determined that the maturity level of DOT's Configuration Management domain is Level 2: *Defined*. We noted that DOT has 12 open prior-year recommendations in the Configuration Management domain[31] that relate to improving its vulnerability management program and establishing baseline deviations and implementing oversight for improving the change control process.

In addition, we continued to identify vulnerabilities present on the DOT Common Operating Environment (COE) and in a sample of DOT and FAA systems that (1) DOT and FAA did not remediate timely, (2) were not compliant with established configuration baselines, (3) did not have fully developed configuration management plans, and (4) did not have appropriately maintained configuration change request documentation.

The following sections detail the weaknesses we noted in DOT's configuration management controls.

Vulnerability Management Program and Processes

Independent vulnerability scans of DOT's COE environment and a sample of DOT and FAA 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 were significantly overdue for remediation. Furthermore, some of the vulnerabilities identified were included in the Cybersecurity and Infrastructure Security Agency's (CISA's) Known Exploited Vulnerabilities (KEVs) listing, and DOT did not remediate them within the defined timeframe. Finally, we were able to exploit some of the identified vulnerabilities—along with other penetration testing techniques—to compromise the COE environment.

[31] See Appendix C for additional information regarding these prior-year recommendations.

As part of our penetration testing, the assessment team was able to exploit vulnerabilities due to inconsistent application of password policies and misconfigured and unpatched systems to obtain unauthorized elevated user permissions/privileges and access system resources. DOT's Security Operations Center was alerted to some of the activities performed during the penetration test but did not take action because they were made aware it was an approved test.

DOT has not consistently implemented its vulnerability remediation and management processes. Unsupported operating systems, unpatched applications, and configuration weaknesses existed without adequate protection such as the timely implementation of patches or compensating controls. In addition, DOT has not implemented adequate system and application configurations such as using strong authentication methods to minimize security risks. Further, DOT inconsistently applied its password policy by allowing the use of default passwords, factory-setting passwords, and/or simple passwords that did not meet the complexity requirements set by password policies.

DOT's *Cybersecurity Compendium Supplemental: DOT Cybersecurity and Privacy Control Baselines and Organization Defined Parameters (ODP) NIST 800-53 Rev. 5* (October 2023), control RA-5, Vulnerability Monitoring and Scanning, requires DOT to remediate legitimate vulnerabilities based on the vulnerability criticality, source, and the *DOT Security Weakness Management Guide*, in accordance with an organizational assessment of risk. Furthermore, the *DOT Cybersecurity Compendium* includes additional controls to further prevent exploitation attempts.

In addition, DHS requires Federal agencies to remediate KEV vulnerabilities in accordance with the timelines set forth in the CISA-managed vulnerability catalog.[32]

The inconsistent application of vendor patches could jeopardize the integrity and confidentiality of DOT's sensitive information. Without remediating all significant security vulnerabilities, systems could be compromised, resulting in potential harm to DOT's data confidentiality, integrity, and availability.

If a malicious actor compromises an account with elevated privileges, such as the account of a system administrator, the magnitude of harm increases, as the attacker can upload malware, steal sensitive data, add or delete users, change system configurations, and alter logs to conceal his or her actions.

Further, unauthorized users can leverage unnecessary elevated user permissions and privileges to systems and data to compromise and access system resources. Poor password controls and weak application/enforcement of DOT's password policies may lead to unauthorized access of systems and data.

Baseline Configurations

To facilitate the implementation of standardized baseline security configuration policies and procedures, DOT component officials are responsible for ensuring that DOT only uses approved configuration settings for any product deployed in the information system. Further, the DOT Chief Information Security Officer must approve any deviations from the approved configuration

[32] Binding Operational Directive 22-01, *Reducing the Significant Risk of KEVs.*

settings.[33] However, based on a review of baseline configuration compliance reports for DOT and FAA systems, we noted that systems were not compliant with configuration standards set by DOT policy.

This issue occurred because DOT and FAA have not completed the documentation of their systems' required baseline configuration deviations and obtained associated approvals for those baseline deviations.

Without complying with baseline configurations, DOT is at risk of having misconfigured and insecure systems on the network. These misconfigured and insecure systems make it difficult for the Department to ensure its information systems are adequately secured and protected and place the systems and the Department at risk for compromise.

Configuration Management Plans

We noted weaknesses in the effectiveness of configuration management plans for four of the seven FIPS 199 high-risk systems tested. DOT either had not developed configuration management plans for the sampled systems, or the plans were not current or were missing key components.

FAA management did not believe it was required to obtain approval for one system's changes by a configuration control board, as the changes would not impact other FAA systems. However, the system's System Characterization Document (December 2022) indicated that the system is connected to other FAA systems residing in other domains. In addition, FAA indicated that one system is comprised of commercial-off-the-shelf components that has a baseline configuration maintained by the DHS CDM contract implementer. The FAA manages changes to each component and must develop a system-level configuration management plan to specify requirements for each component, including their configuration management processes. Further, FAA is updating the configuration management plan for one other system, with a planned completion date of Quarter 4 2024.

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

Change Management Procedures

We noted weaknesses in the effectiveness of FAA and OST Infrastructure and Operations (I&O) change management controls based on the test results for a sample of 25 changes selected from 5 FIPS 199 high-risk systems tested. Specifically, FAA and OST I&O did not consistently implement change management procedures for authorizing, documenting, testing, and conducting a post-implementation audit of system changes.

The Department has not implemented oversight of configuration change activities to ensure that DOT and OAs properly document configuration changes to their information systems, track the changes through implementation, and perform a post-implementation review to verify that configuration management personnel are following procedures. In addition, DOT's OST did not provide requested evidence for a sample of changes selected during the audit period.

[33] *Cybersecurity Compendium Supplemental: DOT Cybersecurity and Privacy Control Baselines and ODP NIST 800-53 Rev. 5* (October 2023), security control CM-6, Configuration Settings.

DOT's *Cybersecurity Compendium Supplemental: DOT Cybersecurity and Privacy Control Baselines and ODP NIST 800-53 Rev. 5* (October 2023), control CM-3, Configuration Change Control, requires DOT and the OAs to authorize, document, and test changes before implementing them in the environment, as well as to audit the changes after implementing them.

FAA's Order 1370.121B, *FAA Information Security and Privacy: FAA Implementation of NIST Controls Supplemental Implementing Directive* (May 10, 2023), control CM-3, Configuration Change Control, requires FAA to authorize, document, and test changes before implementing them in the environment, as well as to audit the changes after implementing them.

Without proper documentation of configuration change requests, individuals could make unauthorized configuration changes to DOT and/or FAA systems. Unauthorized changes could weaken the security posture or impact availability of systems operated by DOT and FAA.

Identity and Access Management

An agency with an effective identity and access management program ensures that all privileged and non-privileged users use strong authentication for accessing organizational systems; employs automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its identity, credential, and access management program.

We determined that the maturity level of DOT's Identity and Access Management domain is Level 2: *Defined.* We found that DOT has opportunities to improve its identity and access management program by implementing the seven open prior-year recommendations in this area.[34] These recommendations relate to continuing efforts to complete overdue background reinvestigations, continued implementation of MFA deployment, and implementation of automated controls for managing user activities.

The following sections detail the weaknesses we noted in DOT's Identity and Access Management controls.

Background Investigations and Reinvestigations

The Office of Personnel Management (OPM) requires DOT to conduct background investigations periodically and when an individual's risk level changes.[35] However, we noted that the FAA did not consistently ensure employees had the proper background investigations and reinvestigations in accordance with OPM and FAA policy.[36] Specifically, we noted the following issues:

- Based on our observation of the FAA Investigations Tracking System *FAA Employee Reinvestigation Due Report*, as of June 10, 2024, a total of 8,411 FAA personnel are overdue for a background reinvestigation.
- FAA did not initiate background reinvestigations in a timely manner before they expired. Specifically:

[34] See Appendix C for additional information regarding these prior-year recommendations.
[35] Code of Federal Regulations Title 5, *Administrative Personnel*, Chapter I, *Office of Personnel Management*, Subchapter B, *Civil Service Regulations*, Part 731 – *Suitability*, Subpart 731.106, *Designation of public trust positions and investigative requirements*.
[36] FAA Order 1600.1F, *Personnel Security Program* (November 4, 2021).

- For 14 out of 25 sampled FAA employees and contractors, FAA did not initiate their background reinvestigation before their current investigation expired. These individuals are not enrolled in continuous evaluation, given their moderate position sensitivity and risk designation.
- For 1 out of 25 sampled new FAA employees and contractors, the individual's background investigation was last conducted in October 2015. FAA Personnel Security incorrectly accepted reciprocity for an individual with a moderate position sensitivity and risk designation. FAA Personnel Security stated that they had addressed this error with the manager and the Personnel Security Specialist.

FAA management stated that the backlog of background reinvestigations is the result of inadequate resources, given ongoing issues with funding and personnel to complete the investigations. Specifically, FAA management stated that, due to an increased workload, including significant hiring surges of FAA personnel, FAA was required to shift resources away from conducting moderate-risk reinvestigations to keep up with agency priorities. FAA expects to have the backlog eliminated by FY 2028.

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

User Authentication

The DOT ITIM 2022-006, *U.S. DOT Implementation Guidance for MFA for Users of Information Systems and Applications* (July 8, 2022), states, "DOT OCIO requires all networks to be MFA compliant by December 31, 2022, and systems to be MFA compliant by December 31, 2023."

Although DOT employees and contractors with network accounts are required to authenticate to the DOT network using a Personal Identity Verification (PIV) card unless an exemption has been granted and approved, we found that the Department has not transitioned all of its information systems (e.g., major applications and GSS) to MFA.

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

Based on our review of the CSAM report of 461 DOT FISMA-reportable systems in operational status (as of June 11, 2024):

- DOT has not yet implemented MFA for 161 systems. The CSAM report either shows the MFA status for these systems as "still planned" or does not show an MFA status.
- DOT has not yet implemented MFA for 43 of 150 systems that collect, manage, or maintain Social Security Numbers.
- DOT identified 14 systems as high-value assets (HVA). Of those systems:
  - DOT has not implemented MFA for internal users for seven systems.
  - DOT has not yet implemented MFA for external users for six of the nine HVA systems that have external users.

As a result, DOT has not met either its ITIM 2022-006 target goal of 100 percent MFA compliance for all systems by December 31, 2023, or its projected implementation rate of 95 percent MFA compliance.

DOT management stated that MFA compliance target goals did not account for the complexity of some systems, system modernizations and upgrades needed, and implementation of privileged access solutions. DOT management also stated that MFA compliance rates are expected to be affected by the recent inclusion of OT systems for FISMA MFA reporting, as required by DHS CISA guidance in May 2024, as efforts continue in DOT's identification of OT systems and conversion of those systems to utilize MFA.

DOT OCIO noted that it will continue to work with the OAs and system owners that have non-compliant systems to achieve MFA compliance by providing assistance, including expediting solutions wherever possible and feasible. In addition, OCIO will work with OAs to ensure OCIO updates CSAM to reflect the current MFA compliance statistics.

Weaknesses related to authentication mechanisms make it difficult for DOT to ensure that it has adequately secured and protected its information systems and places the systems and the Department at risk for compromise. Specifically, the lack of mandatory MFA use means information systems are more susceptible to attacks on user accounts.

Privileged User Account Management

DOT policy[37] requires an annual review to validate assigned privileges and to reassign and remove privileges to correctly reflect the organizational mission and business needs. In addition, FAA policy[38] requires the review and analysis of system audit records for indication of compromise, such as unauthorized access, unauthorized account additions or role modifications, and misuse of authority or access. However, DOT has not effectively managed and reviewed privileged user accounts (and related activities). Specifically, for a sample of in scope high-impact[39] and moderate-impact[40] information systems, we noted the following:

- The COE system owner did not conduct periodic event logging audit review, analysis, and reporting of privileged user account activities.
- For one system, DOT did not provide documentation supporting account recertification procedures, privileged account recertification reviews, and event logging and the periodic review, analysis, and reporting of privileged user account activities.
- FAA has not enabled audit logging of privileged user activities for one sampled high-risk system and two sampled moderate-risk systems. Furthermore, for these three sampled FAA systems, we found that:
    - FAA had not conducted periodic privileged user account reviews for one of the systems.

[37] *DOT Cybersecurity Compendium Supplemental: DOT Cybersecurity and Privacy Control Baselines and ODP NIST 800-53 Rev. 5* (October 2023), security controls AC-6(7), Least Privilege | Review of User Privileges; AU-6, Audit Record Review, Analysis, and Reporting; and AU-6(1), Audit Record Review, Analysis, and Reporting | Automated Process Integration.
[38] FAA Order 1370.121B, *Information Security and Privacy: FAA Implementation of NIST Controls Supplemental Implementing Directive*.
[39] FIPS Publication 199 – *Standards for Security Categorization of Federal Information and Information Systems* defines the potential impact as high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
[40] FIPS Publication 199 defines the potential impact as moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

  - Although FAA has developed account recertification procedures, it did not provide evidence supporting that it conducted a privileged account recertification review for two of the systems.

- Although FAA is logging privileged user account activities, it did not provide evidence to support that it reviewed and monitored these logs for one sampled high-risk system and one sampled moderate-risk system.

The *COE System Security Plan*, version 6.1.1 (September 2023), control AU-6, Audit Record, Review, Analysis, and Reporting, is a planned control, and the OST I&O has not yet defined the requirements for event logging audit review, analysis, and reporting for the COE.

Furthermore, these weaknesses resulted from various causes, including lack of documented account management procedures, inadequate identification of privileged user roles so that DOT can isolate and monitor their activities, and documentation that did not demonstrate that DOT had implemented procedures for managing and monitoring privileged accounts.

Because privileged roles are assigned to individuals to enable them to perform certain security-relevant functions that ordinary users are not authorized to perform, the inadequate assignment of—and infrequent review and monitoring of—these privileged roles increase the risk of a lack of accountability and account misuse that could violate DOT's information systems parameters.

Data Protection and Privacy

An agency with an effective data protection and privacy program maintains the confidentiality, integrity, and availability of its data; can assess its security and privacy controls, as well as its breach response capacities; and reports on qualitative and quantitative data protection and privacy performance measures.

We determined that the maturity level of DOT's Data Protection and Privacy domain is Level 2: *Defined.* We noted that DOT has six open prior-year recommendations in this area related to implementing encryption of data at rest and in transit, as well as monitoring the effectiveness of computer media sanitization.[41]

We noted that the implementation of data protection and privacy controls was not effective across DOT with regard to data exfiltration, encryption of sensitive data, and data breach response testing. Specifically, we noted the following:

- DOT has not fully implemented controls (such as blocking sensitive data from being copied to a removable media device) to restrict the transference of PII and other sensitive data. Currently, default security portal policies provide limited DLP features; however, they do not prevent or restrict data extraction. DOT's rollout of DLP functionality throughout the Department to all endpoints is still ongoing and not complete. In addition, the Department has not provided evidence to demonstrate that it performed data exfiltration exercises.
- DOT has not developed its plans for encrypting data in transit using encrypted Domain Name Service and enforcing Hypertext Transfer Protocol Secure (HTTPS) for all production HTTP traffic, in accordance with OMB M-22-09, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*, issued on January 26, 2022, and Executive Order 14028*, Improving our Nation's Cybersecurity*, issued on May 12, 2021.

[41] See Appendix C for additional information regarding these prior-year recommendations.

- Although DOT required the OAs to be fully compliant with DOT's ITIM-2022-004, *U.S. Department of Transportation Data Encryption Guidance*, issued on April 4, 2022, by the end of calendar year 2022, with regard to the encryption of data at rest and in transit, the OAs did not meet this deadline. Specifically, based on our review of the CSAM system report covering all operational FISMA-reportable systems on February 22, 2024, we noted the following:
  - 18 of 35 high-risk DOT systems that store sensitive data, or 51.4 percent, do not encrypt data at rest, and 21 of the 35 systems, or 60 percent, do not encrypt data in transit.
  - 101 of 308 moderate-risk DOT systems, or 32.8 percent, do not encrypt data at rest.
  - 118 of 308 moderate-risk DOT systems, or 38.3 percent, do not encrypt data in transit.
- Although DOT has defined and communicated its data breach response plan and established a breach assessment and response team, DOT did not provide evidence that it tested the breach response plan in FY 2024, as required by DOT Order 1351.19, *PII Breach Notification Controls*. The Chief Privacy Officer indicated that an actual breach (or major incident) occurred in May 2023; however, DOT did not provide artifacts such as an after-action report, reports, timelines, and credit monitoring actions related to data breach response.

DOT attributed these weaknesses to its ongoing efforts related to the encryption of data at rest and in transit. In addition, FAA management stated that it will be able to block individuals from copying sensitive data to a removable media device once DOT has fully deployed the endpoint tool to its endpoints. DOT management stated that they are still in the process of fully implementing the encryption of data at rest and in transit. DOT expects to reach a target of 92 percent for data-in-transit capabilities by the end of FY 2024.

If DOT does not physically disable or remove unused connection ports and input/output devices, they are at an increased risk of data exfiltration and the introduction of malicious code through those ports or devices. Without the implementation of data encryption, there is an increased risk of unauthorized disclosure or modification of sensitive data. Further, without testing its breach response plan, DOT cannot ensure that it can effectively respond to cybersecurity incidents, increasing the risk to sensitive data.

Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities; measures the effectiveness of its security awareness and training program; and ensures staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

We determined that the maturity level for DOT's Security Training domain is Level 2: *Defined*. We noted that DOT has three open prior-year recommendations in this area related to tailoring security awareness training policy to DOT's unique environment and verifying that personnel performing certain security-related roles receive specialized training.[42]

[42] See Appendix C for additional information regarding these prior-year recommendations.

We noted that DOT has not developed a current workforce assessment, that privileged users have not consistently completed RBT, and that new users have not completed SAT, as required. Specifically, we noted the following conditions related to security training:

- The *DOT Cybersecurity Workforce Management Program* (January 5, 2017) states that "DOT and Components are expected to develop an annual assessment of their workforce"; however, we noted that DOT last conducted a workforce assessment and prepared action plans on February 13, 2019. The Department noted that it is currently in the process of conducting an assessment of the entire IT workforce and that the cybersecurity workforce will be part of that effort.
- Of the 440[43] privileged users identified in the Department's *SAT-RBT Completion FY23*[44] report (March 4, 2024), 374, or 85 percent, completed RBT in FY 2023, compared to the overall target completion rate of 95 percent. Specifically, in-scope OAs[45] and their RBT completion rate ranged from 66.7 to 96.4 percent. In addition, of the 3,483 privileged FAA users, 3,313, or 95.1 percent, completed RBT.
- For 13 of 25 new hires from July to December 2023, or 52 percent, DOT has no record of the employee completing cybersecurity and privacy literacy training.

Management stated that DOT uses the application DOT Learns to track DOT personnel cyber security workforce roles and that DOT has developed a workforce management dashboard where this data is aggregated. However, management noted that there are deficits, particularly at the contractor level. Specifically, because DOT has not yet implemented a process to determine contractor classification for its cybersecurity workforce.

Management also stated that deficiencies in RBT for privileged users may have occurred because DOT Learns lacks the functionality to record the designation of "Privileged User" and privileged users do not have a means to self-identify as a "Privileged User." Management intends to develop a specific rules of behavior and an acceptable use policy whereby privileged users will attest to their role as a privileged user and DOT will track them accordingly and provide the prerequisite training for their role. DOT is still in the process of implementing this initiative, with a roll-out date of 2025.

The *DOT Cybersecurity Training Program Plan, Version 1.0 (*March 10, 2022), requires employees and contractors to complete mandatory cybersecurity and privacy literacy training within 30 days of duty entrance and annually thereafter. Further, it requires all users in roles with significant cybersecurity responsibilities to complete specialized, role-based cybersecurity training specific to assigned roles and responsibilities prior to obtaining access to DOT systems and DOT information or to performing assigned duties, annually thereafter, and when required by system changes.

Without a current cybersecurity workforce assessment, DOT may not onboard, appropriately assign, and train necessary security personnel to perform the required security functions, which may pose a security risk to DOT's IT environment. In addition, employees and contractors that have not completed annual security awareness and role-based training are more likely to be

[43] This number excludes FAA (as we discuss FAA separately) and OAs not in scope.
[44] Given that DOT's cybersecurity training period ends August 31, 2024, and falls outside the FISMA audit period of July 1, 2023, through June 30, 2024, we tested the August 31, 2023, completion statistics, as they fall within the 2024 audit period.
[45] Refer to Appendix D for a list of organizations included in the audit scope.

victim to targeted phishing attempts, malware, and other cyberattacks, which poses a risk to DOT's sensitive data and systems.

Recommendations:

We recommend that the DOT CIO take the following actions, in addition to addressing the prior-year open recommendations[46] related to the weaknesses noted for the Protect function:

3. Enforce password polices to ensure passwords are harder to guess and extend the timeframe in which individuals can enter the next password. Further, use cryptographically protected channels to transmit passwords.

4. Document and implement procedures to review on a periodic basis users with administrative rights and privileged groups with access to domain controllers.

5. Implement protections to restrict access to system tools used to create and manage shadow copies of the hard drive.

6. Document and implement procedures to analyze user account passwords against lists of commonly used and compromised passwords and require users to reset weak or compromised passwords.

7. Direct the DOT Information Assurance and Privacy Management Office and Breach Assessment and Response Team to implement annual testing of the Breach Notification Controls, as required by DOT Order 1351.19, *Personally Identifiable Information Breach Notification Controls*.

8. Complete the DOT workforce assessment, which includes the entire DOT IT and cybersecurity workforce.

[46] See Appendix C for additional information regarding these prior-year recommendations. Prior-year FISMA open recommendations related to the findings noted within the "Protect" function: Recommendations 5 and 8 (DOT OIG Report Number FI2018017, January 24, 2018); Recommendations 6 and 8 (DOT OIG Report Number FI2019023, March 20, 2019); Recommendations 5, 6, and 7 (DOT OIG Report Number QC2020002, October 23, 2019); Recommendations 2, 4 through 6, 8, and 9 through 13 (DOT OIG Report Number QC2021003, October 26, 2020); Recommendations 3 through 5 (DOT OIG Report Number QC2022006, October 25, 2021); Recommendations 2 through 7 (DOT OIG Report Number QC2022042, September 28, 2022); and Recommendations 1 and 2 (QC2023047, September 27, 2023). We are not repeating these recommendations within this report.

Security Function: Detect

The objective of the Detect function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events[47] include anomalies and changes in the organization's IT environment that may impact organizational operations, including mission, capabilities, or reputation. We determined that the maturity level of DOT's Detect function is Level 2: *Defined.*

Information Security Continuous Monitoring

An agency with an effective ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program in delivering persistent situational awareness across the organization; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

We determined that the maturity level for DOT's ISCM domain is Level 2: *Defined.* We noted that there are three open prior-year recommendations in this area related to establishing agreements to delineate responsibilities for the COE common controls with the OAs and conducting an annual cybersecurity performance analysis review.[48]

In addition, we identified the following weaknesses related to ISCM:

- For 21 of 61 sampled systems, or 34.4 percent, OAs did not perform the Security Control Assessment (SCA) on an annual basis or did not provide evidence to support that it performed the SCA (FAA, FMCSA, MARAD and OST). Based on our sample, we estimate[49] that OAs did not perform or did not document performance of SCAs for 167 of 443 systems, or 37.8 percent.[50]
- For 11 of 61 sampled systems, or 18 percent, either OAs did not provide ISCM documentation, or the ISCM documentation was not current or did not include a control assessment schedule (FAA, MARAD, and OST). Based on our sample, we estimate that OAs did not provide ISCM documentation or did not provide ISCM documentation that was current or did not include a control assessment schedule for 86 of 443 systems, or 19.3 percent.[51]

As noted in the Risk Management section above, these SA&A and ISCM deficiencies are attributed to a variety of causes, such as (1) OAs allowing some assessment and authorization documentation to expire due to the absence of an ATO package, and (2) changes to the system's environment.

[47] https://csrc.nist.gov/glossary/term/cybersecurity_event
[48] See Appendix C for additional information regarding these prior-year recommendations.
[49] We performed an extrapolation of selected results to the population of 443 systems. These extrapolated estimated error rates took into consideration the stratification of the system sampled to derive the weighted point estimate of the error rate, with a 90 percent confidence level. Consequently, the weighted error rates are not equal to the ratio of errors observed during the audit divided by 61, the system sample size. Please refer to Appendix B: Objective, Scope, and Methodology of this report, which further describes the system selection methodology.
[50] Our 37.8 percent estimate has a margin of error of +/- 10 percentage points at the 90 percent confidence level.
[51] Our 19.3 percent estimate has a margin of error of +/- 8.4 percentage points at the 90 percent confidence level.

DOT policies[52] require system owners to develop a strategy for continuous monitoring of information systems, including assessing all security controls—including volatile controls—implemented at the system level, at a frequency dictated by DOT. Furthermore, DOT policies require OAs to assess security controls and prepare a SAR to document the issues and findings.

Without assessing the effectiveness of system security controls on a continuous basis, DOT does not have reasonable assurance that controls are operating effectively, which may expose the Department to information loss, fraud, or abuse. In addition, the lack of adequate, timely assessments and/or continuous monitoring limits authorizing officials' ability to make effective decisions regarding the risk for compromise created by system operations.

Recommendations:

Prior FISMA recommendations[53] related to the weaknesses noted in the Detect function remain open. We are not making any new recommendations.

[52] DOT *Security Authorization & Continuous Monitoring Performance Guide*, Version 4.2 (September 2019), and FAA *Fiscal Year 2024 Security Authorization Handbook,* Version 1 (October 2023).
[53] Prior FISMA open recommendations related to the findings noted within the "Detect" function: Recommendations 2, 5 and 10 (DOT OIG Report Number FI2019023, March 20, 2019). We are not repeating these recommendations within this report.

Security Function: Respond

The objective of the Respond function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. We determined that the maturity level of DOT's Respond function is Level 3: *Consistently Implemented*.

Incident Response

An agency with an effective incident response program:

- Uses profiling techniques to measure the characteristics of expected network and system activities so it can more effectively detect security incidents.
- Manages and measures the impact of successful incidents.
- Uses incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.
- Consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.

We determined that the maturity level of DOT's Incident Response domain is Level 3: *Consistently Implemented.* DOT has developed incident response policies and procedures. However, it has not updated its incident response plans to address lessons learned from a major incident and did not meet EL requirements, as noted below. DOT has no open prior-year recommendations in this domain.[54]

The following sections detail the weaknesses we noted in DOT's Incident Response controls.

Incident Response Plan

DOT did not update the OCIO *Cybersecurity Incident Response Plan* (July 2020) on an annual basis or to reflect lessons learned from a recent incident. Specifically, DOT experienced a major incident during FY 2023; however, it has not yet incorporated the lessons learned as documented in the After-Action Report (AAR) (September 11, 2023) into the DOT OCIO *Cybersecurity Incident Response Plan*. For example, the AAR recommended enhancements included defining members and roles for the OCIO core incident response team and improving continuous monitoring, response, escalation, remediation, and reporting standards.

The OCIO *Cybersecurity Incident Response Plan* requires DOT to perform a full review of the incident response plan annually to ensure its relevance and operational effectiveness. However, the Revision History and Approval table does not support that DOT has conducted annual reviews, as it shows that DOT conducted the last review on July 2, 2020. DOT management indicated that the OCIO *Cybersecurity Incident Response Plan* is scheduled for a comprehensive update by September 1, 2024.

[54] See Appendix C for additional information regarding these prior-year recommendations.

Additionally, the Department has not yet completed its review of the incident AAR and will consider potential updates to the existing incident response plan to address any identified gaps or improvements.

Without an up-to-date incident response plan, there is an increased risk that DOT may not adequately record, track, investigate, or resolve security incidents and that personnel may not be aware of their responsibilities. In addition, failure to incorporate lessons learned from major security incidents into incident response plans increases the risk that the plans may be outdated, and that DOT may not implement necessary changes to the plans.

Event Logging

OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), requires Federal agencies to improve their investigative and remediation capabilities to ensure that enterprise security operations centers have centralized access to—and visibility into—system logs. DOT assessed its EL maturity against the requirements in OMB M-21-31 and reported its current EL maturity level as EL0,[55] or not effective.

DOT has not issued policy, implementation instructions, procedures, and configuration guidance to support Departmental enterprise EL to reach the EL1,[56] EL2,[57] and EL3[58] maturity levels by OMB's required due dates in accordance with OMB M-21-31. Additionally, DOT did not meet the following deadlines:

- Within one year of the date of OMB M-21-31, or by August 27, 2022, achieve the EL1 maturity level.
- Within 18 months of the date of OMB M-21-31, or by February 27, 2023, achieve the EL2 maturity level.
- Within two years of the date of OMB M-21-31, or by August 27, 2023, achieve the EL3 maturity level.

In addition, we noted that FAA's OMB M-21-31 status report for EL (dated February 1, 2024), showed that several logging categories had completion percentages below 100 percent for EL1 (Basic). Furthermore, FAA's quarterly CIO FISMA metrics submission to the Department also reports that FAA is at EL0.

DOT has not issued policy, implementation instructions, procedures, and configuration guidance to support Departmental enterprise EL in accordance with OMB M-21-31. DOT management indicated that DOT plans to issue this documentation by September 30, 2024. Further, FAA management indicated that FAA has not yet achieved completion percentages of 100 percent for EL1 for all logging categories.

[55] Per OMB M-21-31, EL0 maturity level signifies that the organization either has not met or has only partially met the logging requirements of highest criticality. See OMB M-21-31 online at https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.
[56] Per OMB M-21-31, EL1 maturity level signifies only the logging requirements of highest criticality are met.
[57] Per OMB M-21-31, EL2 maturity level signifies logging requirements of highest and intermediate criticality are met.
[58] Per OMB M-21-31, EL3 maturity level signifies logging requirements at all criticality levels are met.

Cyberattacks underscore the importance of increased government visibility before, during, and after a cybersecurity incident. Information from logs on Federal information systems (for both on-premises systems and connections hosted by third parties, such as cloud service providers) is invaluable in detecting, investigating, and remediating cyber threats. By not achieving the EL1 and EL2 maturity levels, DOT is not meeting logging requirements of the highest criticality. DOT is currently at the EL0 maturity level; as such, its EL capabilities are not effective based on OMB M-21-31. Further, DOT may not be able to correlate audit log records across different repositories in a complete or risk-based manner, as defined by OMB M-21-31, which may increase the risk that DOT may not collect all meaningful and relevant data on suspicious events. This may, in turn, increase the risk that DOT may inadvertently miss the potential scope or veracity of suspicious events or attacks.

Recommendations:

We recommend that the DOT CIO take the following actions:

9. Update the OCIO *Cybersecurity Incident Response Plan* to incorporate lessons learned from the security incident and ensure that it reviews and updates the plan annually.

10. Document and implement a plan to issue policy, implementation instructions, procedures, and configuration guidance to support Departmental enterprise EL in accordance with OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.*

Security Function: Recover

The objective of the Recover function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services that have been impaired due to a cybersecurity incident. The Recover function supports the timely recovery of normal operations to reduce the impact of a cybersecurity incident, including recovery planning, improvements, and communications. We determined that the maturity level of DOT's Recover function is Level 2: *Defined*.

Contingency Planning

An agency with an effective contingency planning program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures regarding the effectiveness of information system contingency planning program activities.

We determined that the maturity level for DOT's Contingency Planning domain is Level 2: *Defined.* We noted that DOT has three open prior-year recommendations in the Contingency Planning domain[59] related to conducting oversight to ensure DOT develops, updates, and tests contingency planning documentation in a timely manner and ensuring that DOT describes alternate processing sites in the contingency plan.

DOT has not consistently implemented contingency planning processes. For the sample of DOT systems within scope across the OAs, we noted weaknesses related to the development, maintenance, and testing of contingency plans; maintenance of BIAs; identification of alternate storage or processing sites; and data backups. Specifically, we noted the following:

- For 21 of 61 sampled systems, or 34.4 percent, we noted weaknesses in contingency plan testing. Based on our sample, we estimate that OAs did not perform or did not document performance of contingency plan testing for 166 of 443 systems, or 37.4 percent.[60] Specifically, we noted the following:
    - For 16 of 61 sampled systems, or 26.2 percent, OAs did not provide evidence that they performed contingency plan testing (FAA, MARAD, and OST).
    - For 5 of 61 sampled systems, or 8.2 percent, although the OA provided evidence that it had performed contingency plan testing, it did not perform the testing on an annual basis (FAA).
- For 10 of 61 sampled systems, or 16.4 percent, the OA did not provide a BIA (FAA, MARAD, and OST). Based on our sample, we estimate that OAs did not provide a BIA for 76 of 443 systems, or 17.1 percent.[61]
- For 15 of 61 sampled systems, or 24.6 percent, the OAs did not provide an Information System Contingency Plan and National Airspace System (NAS) System Contingency Plan

[59] See Appendix C for additional information regarding these prior-year recommendations.
[60] Our 37.4 percent estimate has a margin of error of +/- 10 percentage points at the 90 percent confidence level.
[61] Our 17.1 percent estimate has a margin of error of +/- 8.5 percentage points at the 90 percent confidence level.

(FAA, MARAD, and OST). Based on our sample, we estimate that OAs did not provide an information system contingency plan for 121 of 443 systems, or 27.3 percent.[62]

- For 4 of 12 sampled FAA GSS, or 33.3 percent, FAA did not identify an alternate storage or processing site.
- For 4 of 12 sampled FAA GSS, or 33.3 percent, FAA did not provide evidence of backups of information at the user and system levels.
- DOT does not review and test its Continuity of Operations Plan (COOP) on an annual basis. The last COOP test that DOT performed was in October 2022.

FAA and OST have open POA&Ms related to contingency planning weaknesses. In some cases, DOT or the OAs did not provide documentation or management did not respond to exceptions communicated.

The Cybersecurity Compendium Supplemental - *DOT Cybersecurity and Privacy Control Baselines and Organization Defined Parameters (ODP)* (October 2023) requires that contingency plans are developed and tested for the system prior to initial ATO and annually thereafter to determine the effectiveness of the plan and the readiness to execute the plan. Further, it requires the establishment of an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions within the timeframes and objectives. In addition, backups of user-level information contained in system components are required to restore full system function and operations via daily incremental and weekly full backups or consistent with identified timeframes and objectives.

Additionally, section 3.2 of NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, indicates that the BIA is a key step in implementing the contingency planning controls in NIST SP 800-53 and in the contingency planning process overall. The BIA's purpose is to correlate the system with the critical mission/business processes and the services provided and based on that information, characterize the consequences of a disruption.

Effective contingency planning and comprehensive testing are crucial to ensure organizational systems and data are available and IT systems and applications are resilient against outages and disruptions. Failure to comprehensively test and exercise documented plans increases the risk that DOT will not effectively identify weaknesses or areas of improvement in preparation for real-world contingency events.

In addition, if DOT does not identify alternate storage sites or alternate processing sites, there is a risk that backups will be subject to the same risks as the primary site. Also, if DOT does not maintain data backups, this may delay or prevent the timely restoration of data upon system recovery.

Recommendations:

Prior FISMA recommendations[63] related to the weaknesses noted in the Recover function remain open. We are not making new recommendations.

[62] Our 27.3 percent estimate has a margin of error of +/- 10.1 percentage points at the 90 percent confidence level.
[63] Prior FISMA open recommendations related to the findings noted within the "Recover" function: Recommendations 16 and 17 (DOT OIG Report Number QC2021003, October 26, 2020) and Recommendation 8 (DOT OIG Report Number QC2022042, September 28, 2022). We are not repeating these recommendations within this report.

IV. CONCLUSION

DOT relies on hundreds of information systems to carry out its mission of "serving the American people and economy through the safe, efficient, sustainable, and equitable movement of people and goods," including safe air traffic control operations and stewardship of billions of taxpayer dollars. The effectiveness of DOT's cybersecurity program is critical to ensuring these systems, their core functionality, and the underlying data assets are not compromised by malicious actors exploiting system risks and vulnerabilities and thereby jeopardizing citizen safety and taxpayer dollars.

Although DOT has devoted significant effort and resources to meeting the demands of new and changing regulatory requirements and enhancing its security program—necessitated by evolving technology and newer, more sophisticated threats—DOT's security program remains at the "Defined" level of maturity. This is due to unaddressed deficiencies pervasive across the FISMA areas of DOT's security program. These deficiencies can be attributed to the inconsistent enforcement of an enterprise-wide information security program, ineffective communication and information exchange between the Department and mission and the technologically diverse OAs, and DOT's inability to manage significant security risks and remediate prior-year recommendations.

DOT has made steps toward improving its current cyber security program, including employing dedicated resources, and initiating a framework to address prior-year deficiencies, with conscientious efforts to continuously refine its processes to ensure that they will be sustainable and repeatable. DOT has currently implemented a tactical approach to addressing prior-year deficiencies. However, DOT has not yet developed a long-term strategy. The DOT CIO is in the process of developing a cyber strategy that should include a discussion of DOT's risk tolerance and how it plans to assess, respond to and monitor risks.

DOT is also in the midst of change and process improvements in various program areas. Some of these changes include hiring additional personnel to modernize outdated processes and technology and strengthen DOT's security posture. DOT has made some progress to further implement technology to secure its systems and data, such as MFA. In addition, DOT has plans to implement and offer additional services (such as vulnerability scanning capabilities to OAs) as part of its vulnerability management program to address technical vulnerabilities. However, DOT has not yet formalized this new program.

DOT should continue to assess its current state of security against its defined optimal security program design and security posture. DOT should identify critical risks, flaws, and deficiencies (considering POA&Ms and prior-year audit recommendations), prioritize them in coordination with IT/security leadership and management at the Department and each of the OAs, and remediate them accordingly. DOT should ensure that it implements its tailored system of internal controls, a structured continuous monitoring program with effective communication of security directives, exchange of information, and accountability of the Department and OAs' adherence to enterprise-wide strategic and tactical security responsibilities. DOT should continue to prioritize remediation of critical security flaws to limit risk exposure aligned with the internal controls program. Finalization of the DOT CIO's cyber strategy should assist with closing the gap in DOT's security posture.

V. Agency Comments and Sikich's Response

We provided DOT with our draft report on August 8, 2024, and received DOT's response on August 28, 2024, which is included in its entirety as an appendix to this report. In its response, the Department described that OCIO remains dedicated to improving DOT's Cybersecurity Program and continues to prioritize cybersecurity efforts across the Department. Management indicated that with high-level executive support, DOT has maintained steady progress on many fronts that align with the directives outlined in Executive Order 14028 and began new efforts and made investments in consideration of evolving CISA guidance and capabilities. These efforts include updating DOT's Cybersecurity Compendium and publishing a series of IT Memoranda, holding daily coordination meetings on cybersecurity operations, and continuing to invest in DOT's workforce by enhancing cybersecurity training.

DOT concurs with all 10 recommendations as written and plans to implement these recommendations by August 31, 2025. Therefore, we consider recommendations 1 through 10 resolved but open pending completion of planned actions.

Actions Required

We consider recommendations 1 through 10 resolved but open pending completion of planned actions.

APPENDIX A: BACKGROUND

Federal Information Security Modernization Act of 2014

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. Agencies must also report annually to the OMB and to congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide the minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with FIPS issued by NIST. In addition, NIST develops and issues SPs as recommendations and guidance documents.

FISMA Reporting Requirements

OMB and DHS annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the methodology for conducting FISMA evaluations and the processes for federal agencies to report to OMB and, where applicable, DHS. The methodology includes the following:

- OMB selected 17 supplemental IG FISMA Reporting Metrics that IGs must evaluate during FY 2024, in addition to the 20 core IG FISMA Reporting Metrics that IGs must evaluate annually. The remainder of the standards and controls are evaluated on a 2-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. Beginning in FY 2023, ratings were focused on calculated average scores, wherein IGs would use the average of the metrics in a particular domain to determine the effectiveness of the individual function areas (i.e., Identify, Protect, Detect, Respond, and Recover). OMB encouraged IGs to focus on the calculated average scores of the 20 core IG FISMA Reporting Metrics, as these tie directly to the administration's priorities and other high-risk areas. In addition, the FY 2024 IG FISMA Reporting Metrics indicated that IGs should use the calculated average scores of the supplemental IG FISMA Reporting Metrics and the agency's progress in addressing outstanding prior-year recommendations as data points to support their risk-based determination of the overall effectiveness of the program and function level.

As highlighted in **Table 3**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST Cybersecurity Framework, version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	Risk Management and SCRM
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Implement activities to identify the occurrence of cybersecurity events.	Information Security Continuous Monitoring
Respond	Implement processes to take action regarding a detected cybersecurity event.	Incident Response
Recover	Implement plans for resilience to restore capabilities or services impaired by a cybersecurity event.	Contingency Planning

Source: Sikich's analysis of the NIST Cybersecurity Framework and IG FISMA Reporting Metrics.

The foundational levels of the maturity model in the IG FISMA Reporting Metrics 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** below 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 strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies 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 strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2024 IG FISMA Reporting Metrics

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine the effectiveness of DOT's information security program and practices in accordance with GAGAS and with FISMA.

Scope

We conducted this performance audit in accordance with GAGAS, issued by the Comptroller General of the United States. These 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. OIG contracted with us to conduct the review of DOT's information security program and practices subject to OIG's oversight. Although the OIG is a small component of the Department, based on the number of systems, any testing pertaining to OIG, or its systems does not impair our ability to conduct this mandated audit.

The scope of this performance audit covered DOT's information security program and practices consistent with FISMA and reporting instructions that OMB and DHS issued for FY 2024. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, to support the FY 2024 IG FISMA Reporting Metrics for a sample of 61 systems from a total population of 443 DOT FISMA reportable systems in operation as of November 6, 2023.[64] The sampled systems are broken down by OA as follows: FAA (37), PHMSA (2), OST (6), FHWA (2), FMCSA (2), FRA (2), FTA (2), MARAD (2), NHTSA (4) and OIG (2). We substituted a total of six systems—five for FAA and one for OST Volpe—because we determined that the systems were excluded from testing for reasons such as being retired or being in the process of disposal. Refer to **Appendix E** for the specific systems selected for testing.

In addition, we assessed DOT's technical controls by performing an internal vulnerability assessment and penetration test covering one FAA system, one FRA system, one OST I&O system, and one OST system. These tests included general support systems. We conducted the internal vulnerability assessment and penetration tests to determine the effectiveness of controls that prevent or detect unauthorized access, disclosure, modification, or deletion of sensitive information. We incorporated the results of the internal vulnerability assessment and penetration tests into our FISMA audit results.

The audit also included an evaluation of whether DOT took corrective actions to address open recommendations from prior FISMA audits. Refer to **Appendix C** for the status of prior-year recommendations.

The audit covered the period from July 1, 2023, through June 30, 2024. We performed audit fieldwork from November 2023 to July 2024. **Appendix D** lists the organizations included in the scope of the audit.

[64] We selected a stratified random sample from DOT's population of 443 FISMA-reportable major applications/GSS noted as being in operation to assess DOT's compliance with FISMA.

Methodology

To accomplish our objective, we completed the following procedures:

- Evaluated key components of DOT's information security program and practices, consistent with FISMA and with reporting instructions that OMB and DHS issued for FY 2024.
- Focused our testing activities on assessing the maturity of the 20 core and 17 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Inquired of DOT management and staff.
- Considered guidance contained in OMB's M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a statistical sample of 61 DOT information systems from the 443 systems in DOT's system inventory.
- Analyzed the sample of systems selected for testing, including reviewing selected system documentation and other relevant information, as well as tested selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

DOT's population of systems included 458 systems as of November 6, 2023. For the purposes of our sample, we included those systems that had a System Operational Status of "Operational" (indicated by marking "Yes" in the "FISMA Reportable" field) and that had a response in the "System Type" field of either "Major Application" or "General Support System." We performed our first stratification based on risk category: High, Moderate, and Low. We performed the second stratification based on OA for the High and Moderate systems. This is because the Low category systems do not pose a significant risk to confidentiality, integrity, or availability, nor do they have a substantial impact on DOT's mission. Our third stratification was to stratify FAA into NAS and Non-NAS. We have separated NAS and Non-NAS systems because they operate under two different control environments and are air gapped. Finally, due to the importance of the COE to DOT operations, we created a separate stratum that only included the COE to ensure it would be selected for testing.

For sample selection purposes, we divided the 443 systems into 16 strata based on the stratification methodology described above. We determined the sample size based on the following two requirements:

1. To ensure adequate coverage of the different OAs, we were required to select at least two systems for each OA. One stratum, OST – High, contained a single system, so that we would sample this system with 100 percent probability. This was to ensure that we would sample the COE system with 100 percent probability, given its high importance. We sampled the remaining strata using a probability level that was proportional to the relative sample size, so that the total sample size would be 61 samples selected.

2. We used a confidence level of 90 percent and an expected margin of error of 10 percent, based on considerations and work completed in the 2023 FISMA audit and the realization that the 2024 population was not substantively different than the 2023 population.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model that continued for the FY 2024 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting Metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages were not automatically rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to administration priorities and other high-risk areas. OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2024 IG FISMA Reporting Metrics guidance[65] to form our conclusions for each Cybersecurity Framework domain and function, as well as for the overall agency rating. Specifically, we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics and progress that DOT has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

We evaluated the effectiveness of DOT's information security program and practices, including with regard to FISMA and related information security policies, procedures, standards, and guidelines, and responded to the FY 2024 IG FISMA Reporting Metrics. Our work did not include assessing the sufficiency of internal controls over DOT's information security program or other matters not specifically outlined in this report.

[65] The FY 2024 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the Cybersecurity Framework domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency's information security program is effective at a calculated maturity level lower than level 4.

APPENDIX C: STATUS OF PRIOR FISMA REPORT RECOMMENDATIONS

The following is the status of open recommendations from prior FISMA reports. We determined the current status of prior-year FISMA open recommendations by reviewing DOT's overall status for prior-year recommendations and testing the effectiveness of DOT's information security program and practices covering the period from July 1, 2023, through June 30, 2024.

In addition, DOT closed 24 prior-year recommendations during the audit period. Thus, of 71 open recommendations from prior FISMA reports, 47 recommendations remain open as of June 30, 2024.

Prior-Year FISMA Recommendations That Were Closed

2011 FISMA AUDIT, OIG REPORT NUMBER FI2012007
FISMA 2011: PERSISTENT WEAKNESSES IN DOT'S CONTROLS CHALLENGE THE PROTECTION AND SECURITY OF ITS INFORMATION SYSTEM

Number	Recommendation
1b	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.

2013 FISMA AUDIT, OIG REPORT NUMBER FI2014006
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.

2015 FISMA AUDIT, OIG REPORT NUMBER FI2016001
FISMA 2015: DOT HAS MAJOR SUCCESS IN PIV IMPLEMENTATION, BUT PROBLEMS PERSIST IN OTHER CYBERSECURITY AREAS

Number	Recommendation
2	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	Work with FAA to improve its 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	Work with the OAs to ensure they update open POA&Ms with the required data fields.

2016 FISMA Audit, OIG Report Number FI2017008
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.
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.
8	Report/update OST COE security weaknesses found during vulnerability assessments in DOT's Repository (e.g., CSAM) per FISMA, OMB, and DOT requirements.

2017 FISMA Audit, OIG Report Number FI2018017
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.

2018 FISMA Audit, OIG Report Number FI2019023
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 CSAM tool.
3	Develop a process and policy, where applicable, to ensure the Department develops and maintains a comprehensive and accurate inventory of cloud systems, contractor systems, and websites that the public can access.
7	Update specialized training guidance in DOT Cybersecurity Action Memos policy and DOT Cybersecurity Compendium policy to clearly define requirements.
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.

2019 FISMA Audit, OIG Report Number QC2020002
FISMA 2019: DOT's Information Security Program and Practices

Number	Recommendation
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.

2020 FISMA AUDIT, 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.
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.
7	Work with the FAA CIO to complete the revision of FAA Order 1800.66, Configuration Management Policy.
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 ISCM Plan for National Airspace System (NAS) and Mission Support (MS) Systems to ensure the FAA ISCM plan is complete and accurate, making updates as needed.

Prior-Year FISMA Recommendations That Remain Open

NOTE: These remaining open recommendations do not represent—and are not intended to represent—all recommendations that were closed within the respective years or reports identified.

2016 FISMA AUDIT, OIG REPORT NUMBER FI2017008
FISMA 2016: DOT CONTINUES TO MAKE PROGRESS, BUT THE DEPARTMENT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE

Number	Recommendation	Metric Domain Impacted
3	Work with FAA, FHWA, FMCSA, FTA, MARAD, NHTSA, and OST to develop risk acceptance memos for the expired systems identified in this report.	Risk Management
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.	Risk Management
7	Identify and document OST COE compensating controls when used to address security weaknesses in CSAM and system authorizations.	Risk Management

2017 FISMA AUDIT, OIG REPORT NUMBER FI2018017
FISMA 2017: DOT'S INFORMATION SECURITY POSTURE IS STILL NOT EFFECTIVE

Number	Recommendation	Metric Domain Impacted
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.	Identity and Access Management
8	Implement processes verifying that personnel performing certain security related roles receive specialized training needed to meet OCIO guidance.	Security Training

2018 FISMA AUDIT, OIG REPORT NUMBER FI2019023
FISMA 2018: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES

Number	Recommendation	Metric Domain Impacted
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.	Information Security Continuous Monitoring
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.	Risk Management
5	Direct OST to establish Memoranda of Understanding (MOUs) that delineate the responsibilities for COE common controls with each of the following OAs: FHWA, FMCSA, FRA, FTA, OIG, MARAD, SLSDC, and NHTSA.	Information Security Continuous Monitoring
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.	Data Protection and Privacy
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.	Security Training
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.	Risk Management
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.	Information Security Continuous Monitoring
11	Using NIST guidance, test and authorize Continuous Diagnostics and Mitigation (CDM) applications (such as BigFix) that have been placed into operation on DOT's networks without proper security control assessments.	Risk Management

2019 FISMA AUDIT, OIG REPORT NUMBER QC2020002
FISMA 2019: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES

Number	Recommendation	Metric Domain Impacted
1	Perform a review of all POA&M items closed during the audit period to include supporting documentation and re-approve their closure.	Risk Management
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.	Risk Management
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.	Risk Management

Number	Recommendation	Metric Domain Impacted
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.	Risk Management
5	Document OA subnets and OA responsibilities for devices and systems operating on the Common Operating Environment.	Configuration Management
6	Document and implement network segmentation to reduce the attack surface or susceptibility of vulnerable and sensitive OA assets in the Common Operating Environment.	Configuration Management
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.	Identity and Access Management

2020 FISMA AUDIT, OIG REPORT NUMBER QC2021003
FISMA 2020: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES

Number	Recommendation	Metric Domain Impacted
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.	Data Protection and Privacy
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.	Data Protection and Privacy
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.	Identity and Access Management
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.	Configuration Management
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.	Configuration Management
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.	Configuration Management
10	Consolidate to the enterprise Tenable Nessus system to ensure accessibility of baseline compliance and/or vulnerability assessment capabilities.	Configuration Management

Number	Recommendation	Metric Domain Impacted
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.	Configuration Management
12	Document and implement a process to identify software end of life dates and require the development of implementation plans to eliminate unsupported software.	Configuration Management
13	Work with FAA to secure a reliable funding stream for background reinvestigations.	Identity and Access Management
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.	Contingency Planning
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 primary processing capabilities are unavailable, for those systems in accordance with the requirements of the Cybersecurity Compendium and NIST guidance.	Contingency Planning

2021 FISMA AUDIT, OIG REPORT NUMBER QC2022006
FISMA 2021: DOT'S INFORMATION SECURITY PROGRAM AND PRACTICES

Number	Recommendation	Metric Domain Impacted
1	Develop and communicate an organization wide Supply Chain Risk Management strategy and implementation plan to guide and govern supply chain risks.	Supply Chain Risk Management
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.	Risk Management
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.	Configuration Management
4	Work and coordinate with system owners to identify and remediate weak and default authentication mechanisms within their systems and the Common Operating Environment.	Identity and Access Management
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.	Security Training

2022 FISMA Audit, OIG Report Number QC2022042
FISMA 2022: DOT's Information Security Program and Practices

Number	Recommendation	Metric Domain Impacted
1	The Department should ensure that adequate resources are made available and are prioritized to validate the accuracy and completeness of asset inventory counts prior to submission to the Department of Homeland Security (DHS) as part of CIO FISMA Metrics.	Risk Management
2	Coordinate with the components to develop or revise their plans to fully transition the remaining information systems to enable and enforce PIV, except those that are subject to exclusions that are documented and approved.	Identity and Access Management
3	FAA should develop and implement procedures to perform periodic reviews of mobile devices to ensure non-compliant mobile devices are upgraded to the current operating system release.	Configuration Management
4	Strengthen processes to ensure privileged account reviews are completed and privileged account activities are logged and periodically reviewed, in accordance with DOT policy.	Identity and Access Management
5	In coordination with the OA system owners, complete DOT's plans to implement existing solutions where possible and create a plan to address all exceptions where there is not a current solution for encryption of data at rest and in transit.	Data Protection and Privacy
6	In coordination with the OA system owners, complete the deployment of DOT's data loss prevention controls to include the utilization or activation of enhanced DLP features available within existing tools and to develop and implement policies and procedures which eliminate or restrict the ability of users to connect mass storage devices to DOT networks and systems.	Data Protection and Privacy
7	Enhance current procedures to implement and require the retention of records to track when computer media are sanitized prior to disposal or reuse and implement procedures to validate the remediation of computer media that have failed media sanitization upon return to DOT.	Data Protection and Privacy
8	In coordination with the OA system owners, strengthen DOT's oversight of the contingency planning processes to ensure contingency planning documentation is developed, updated, and tested in a timely manner, in accordance with policy.	Contingency Planning

2023 FISMA Audit, OIG Report Number QC2023047
FISMA 2023: DOT's Information Security Program and Practices

Number	Recommendation	Metric Domain Impacted
1	Develop and implement DOT's zero trust architecture plan for network traffic that cannot be routed through traditional TIC access points as required by OMB M-19-26, *Update to the TIC Initiative*.	Configuration Management
2	In coordination with FAA, complete the pilot and testing of TIC 3.0 use cases and revise FAA policies to reflect requirements in OMB M-19-26, *Update to TIC Initiative*.	Configuration Management

APPENDIX D: ORGANIZATIONS VISITED OR CONTACTED

- Office of the Secretary (OST)
- 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 Hazard Materials Safety Administration (PHMSA)

APPENDIX E: REPRESENTATIVE SUBSET OF SAMPLED SYSTEMS BY OPERATING ADMINISTRATION

FAA

#	System Name	Impact Level	Contractor System
1	Enforcement Information System Query and Browse	High	No
2	Airport Surveillance Radar 8 with Common Terminal Digitizer	High	Yes
3	Airport Surveillance Radar Model 9	High	No
4	FAA Continuous Diagnostics and Mitigation	High	No
5	Cybersecurity Test Facility	High	No
6	Delphi Transaction File	Moderate	No
7	Customer Service Center System	Moderate	No
8	ASH External Web Portal	Moderate	No
9	Automated Inventory Tracking System	Moderate	Yes
10	Aeronautical Mobile Communications System	Moderate	Yes
11	En Route Data Distribution System	Moderate	No
12	Low Density Radio Communications Link	Moderate	No
13	Microprocessor En Route Automated Radar Tracking System	Moderate	Yes
14	Terminal Doppler Weather Radar	Moderate	No
15	Wide Area Augmentation System	Moderate	Yes
16	FAA and NTSB Recommendations System	Moderate	No
17	Aeronautical Data Exchange	Moderate	No
18	Aviation Safety Knowledge Management Environment - Enterprise Services	Moderate	No
19	Capitalized Assets Processing	Moderate	Yes
20	IFPA FAA Office of Information Technology (AIT)	Moderate	No
21	Designee Management System	Moderate	No
22	Aviation Insurance Data Management System	Moderate	No
23	Enterprise Information Management Platform	Moderate	Yes
24	Enterprise Services Center - Robotic Process Automation	Moderate	No
25	Tableau	Moderate	No
26	Case and Document Management System	Moderate	Yes
27	UAS Declaration of Manufacturer	Moderate	No
28	Automated Surface Observation System	Low	No
29	FAA Acquisition System Tool	Low	Yes
30	Facility Power Panel System	Low	Yes
31	Next Generation Weather Radar Remote Monitoring Subsystem and On-Site Display	Low	No
32	Air Traffic Services Business Model	Low	Yes

#	System Name	Impact Level	Contractor System
33	Environment and Occupational Safety and Health Training Needs Assessment Tool	Low	No
34	Air Traffic Operations Non-Federal Facilities Web Application	Low	No
35	NAS Common Reference	Low	No
36	Atlas Career Navigator	Low	No
37	Central Server	Low	Yes

OST

#	System Name	Impact Level	Contractor System
1	Common Operating Environment	High	Yes
2	Cyber Security Assessment and Management	High	Yes
3	Departmental Office of Civil Rights General Support System	Moderate	Yes
4	IEC Data Warehouse	Moderate	Yes
5	Railroad Credit Assessment and Portfolio Management System	Moderate	No
6	DOT Acquia Drupal System	Moderate	Yes

FHWA

#	System Name	Impact Level	Contractor System
1	FHWA Organization Information System	Moderate	Yes
2	Fiscal Management Information System 5	Moderate	Yes

FMCSA

#	System Name	Impact Level	Contractor System
1	FMCSA Portal	Moderate	Yes
2	SafeSpect	Moderate	No

FRA

#	System Name	Impact Level	Contractor System
1	Railroad Network System	Moderate	No
2	Railroad Safety Information System	Moderate	No

FTA

#	System Name	Impact Level	Contractor System
1	FTA General Support System	Moderate	Yes
2	Transit Integrated Appian Development Platform	Moderate	Yes

MARAD

#	System Name	Impact Level	Contractor System
1	Mariner Outreach System	Moderate	Yes
2	Comprehensive Academic Management System	Moderate	Yes

NHTSA

#	System Name	Impact Level	Contractor System
1	Drug Recognition Expert	Moderate	Yes
2	Crash Data Acquisition Network	Moderate	Yes
3	Compliance and Enforcement Management System	Low	Yes
4	Traffic Records Improvement Program Reporting System	Low	Yes

OIG

#	System Name	Impact Level	Contractor System
1	US DOT/OIG Infrastructure	Moderate	No
2	Computer Crimes Unit Network	Moderate	No

PHMSA

#	System Name	Impact Level	Contractor System
1	PHMSA Data Mart	Moderate	Yes
2	PHMSA Portal System	Moderate	Yes

APPENDIX F: ACRONYMS

Acronym	Definition
AAR	After Action Report
ATO	Authorization to Operate
BIA	Business Impact Analysis
CDM	Continuous Diagnostics Management
CIO	Chief Information Officer
COE	Common Operating Environment
COOP	Continuity of Operations Plan
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DOT	Department of Transportation
EL	Event Logging
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
HTTPS	Hypertext Transfer Protocol Secure
HVA	High-Value Asset
IG	Inspector General
ISCM	Information Security Continuous Monitoring
I&O	Infrastructure and Operations
IT	Information Technology
ITIM	Information Technology Implementation Memorandum
KEV	Known Exploitable Vulnerabilities
MARAD	Maritime Administration
MFA	Multifactor Authentication
NAS	National Airspace System
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OA	Operating Administration
OCIO	Office of Chief Information Officer
ODP	Organization-Defined Parameters
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of the Secretary
OT	Operational Technology
PHMSA	Pipeline and Hazard Materials Safety Administration
PIV	Personal Identify Verification
POA&M	Plan of Action and Milestones
RA	Risk Assessment
RBT	Role-Based Training

Acronym	Definition
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SAT	Security Awareness Training
SCA	Security Control Assessment
SCD	Security Categorization Document

APPENDIX G: MANAGEMENT COMMENTS

Memorandum

U.S. Department of Transportation
Office of the Chief Information Officer

Subject: INFORMATION: Management Response to Office of Inspector General (OIG) Draft Report – Federal Information Security Modernization Act (FISMA) for Fiscal Year (FY) 2024

From: Kelvin Taylor
Associate DOT Chief Information Officer
Acting Chief Information Security Officer

KELVIN LAMARK TAYLOR

Digitally signed by KELVIN LAMARK TAYLOR
Date: 2024.08.28 16:05:06 -04'00'

To: Kevin Dorsey
Assistant Inspector General for
Information Technology Audits

The U.S. Department of Transportation (DOT or Department) and its Office of the Chief Information Officer (OCIO) remain dedicated to improving DOT's Cybersecurity Program and continue to prioritize cybersecurity efforts across the Department. With high-level executive support, DOT has maintained steady progress on many fronts, aligning with the directives outlined in Executive Order 14028, ***Improving the Nation's Cybersecurity***. The Department also began new efforts and made investments, in consideration of evolving Cybersecurity and Infrastructure Security Agency guidance and capabilities, into enterprise capabilities to further address cybersecurity weaknesses and risks, while continuing to update DOT governing policies and guidance on inventory, cloud adoption, and workforce. DOT's commitment to cybersecurity is evident through the allocation of dedicated resources and the consistent focus on pivotal initiatives during FY 2024. These efforts include:

- Publishing DOT's Cybersecurity Compendium to include Organization Defined Parameters aligned with National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 5, Security and Privacy Controls for Information Systems and Organizations.
- Publishing a series of Information Technology Memoranda to rapidly address departmental issues, communicate management decisions, and establish program and departmental guidance and instructions for compliance with NIST Control and Cybersecurity Framework.
- Continuing to hold daily Cyber Corp coordination meetings on cybersecurity operations, involving both technical experts and leadership representatives from all components within DOT. These meetings provide additional transparency, reporting, and oversight for key processes and initiatives to bolster compliance and align with federal requirements.

- Continuing to invest in DOT's workforce by enhancing cybersecurity training within applications, processes, and deployed capabilities. In FY 2024, OCIO hosted its 8th annual Cybersecurity Symposium with more than 45 training sessions, panels, and presentations. DOT held continual bi-weekly trainings in the Department's Governance Risk and Compliance application, Cyber Security Assessment and Management, and deployed capabilities (i.e., BigFix and Nessus Tenable).

These continued efforts, along with other enhancements, have produced improvements across the enterprise. Based on our review of the draft report, we concur, as written, with OIG's 10 recommendations to assist the Department in further strengthening its information security program. We plan to complete actions to implement all recommendations by August 31, 2025.

We appreciate the opportunity to comment on OIG's draft report. Please contact Willie Crenshaw, Director, FISMA and Compliance, at willie.crenshaw@dot.gov or (202) 202-366-6138 with any questions.

U.S. Department of Transportation
Office of Inspector General

Fraud, Waste, & Abuse Hotline

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