U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

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

OST

Report No. QC2020002

October 23, 2019

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 | QC2020002 | October 23, 2019

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. The act also requires agencies to have annual independent reviews to determine the effectiveness of their programs, and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, we contracted with CliftonLarsonAllen LLP (CLA) to conduct this audit subject to our oversight. The audit objective was to determine the effectiveness of DOT's information security program and practices in five function areas—Identify, Protect, Detect, Respond, and Recover.

What We Found

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

Recommendations

DOT concurs with 1 of CLA's 14 recommendations and partially concurs with the remaining 13 recommendations. CLA considers recommendations 1, 2, 4, 8, 9, 10, 11, and 12 resolved but open pending completion of planned actions. CLA considers recommendations 3, 5, 6, 7, 13, and 14 open and unresolved.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: October 23, 2019

Subject: ACTION: Quality Control Review of the Independent Auditor's Report on DOT's Information Security Program and Practices | Report No. QC2020002

From: Louis C. King
Assistant Inspector General for Financial and 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. The act also requires agencies to have annual independent reviews to determine the effectiveness of their programs, and report the results of these reviews to the Office of Management and Budget (OMB). To meet this requirement, we contracted with CliftonLarsonAllen LLP (CLA), an independent public accounting firm, to conduct this audit subject to our oversight.

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

CLA found that DOT's information security program and practices were not effective. DOT's information security program is at the Defined maturity level, the second lowest level in the maturity model. CLA made 14 recommendations to improve DOT's information security program and practices.

CLA recommends that the Chief Information Officer:

1. Perform a review of all plan of action & milestones (POA&M) items closed during the audit period to include supporting documentation and re-approve their closure.

2. Revise current security weakness management policies and procedures (documenting within a revision history table) to require documented evidence such as calendar appointments, meeting minutes, etc. in support

of POA&M closure decisions to be uploaded into the Cyber Security Assessment and Management system.

3. Work with the Operating Administration (OA) Chief Information Officers (CIO) to review current assessment and authorization processes and implement a validation process to ensure updated security plans, authorizations to operate (ATO) and risk assessments are reviewed and updated to reflect all system (including privacy) controls, vulnerabilities, and that current risks are clearly presented to the authorizing officials.

4. Work with the OA CIOs to develop mechanisms to ensure updated system security plans and assessments of security controls (that were previously assessed as not satisfied or partially satisfied) reflect current operational environments, including an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.

5. Document OA subnets and OA responsibilities for devices and systems operating on the Common Operating Environment.

6. Document and implement network segmentation to reduce the attack surface or susceptibility of vulnerable and sensitive OA assets in the Common Operating Environment.

7. Work with OAs to remediate outstanding identity and access management weaknesses through implementation and closure of POA&Ms and control assessments to determine whether these risks were addressed.

8. Work with component privacy officers to develop and implement procedures then verify the completion, review, tracking and approval through review of updated privacy threshold assessments, privacy impact assessments (PIA), and system of records notices.

9. Document and implement a process to ensure incident response procedures related to the timely notification, reporting, updating, and resolution of security incidents are followed in accordance with policy.

10. Review and update the Office of the Chief Information Officer (OCIO) Cyber Security Incident Response Plan, documenting evidence of review and revisions within a history log.

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.

13. Work with the Office of the Secretary of Transportation's (OST) Office of Intelligence, Security and Emergency Response to ensure the DOT Continuity of Operations Plan (COOP) is reviewed and updated (noting evidence of the review within a history/revision log).

14. Work with the OA CIOs to remediate identified weaknesses in contingency plans and business impact assessments (BIA), such as missing information, lack of timely review, and inadequate approvals, demonstrated by updated contingency plans and BIAs.

DOT concurs with recommendation 10 as written. DOT partially concurs with the remaining 13 recommendations.

We performed a quality control review (QCR) of CLA's report, dated October 8, 2019 (see attachment), and related documentation. Our QCR, as differentiated from an audit engagement performed in accordance with generally accepted Government auditing standards, was not intended for us to express, and we do not express, an opinion on DOT's information security program and practices. CLA is responsible for its independent auditor's report and the conclusions expressed in that report. Our QCR disclosed no instances in which CLA did not comply, in all material respects, with generally accepted Government auditing standards.

We appreciate the courtesies and cooperation of DOT representatives during this engagement. If you have any questions concerning this report, please call me at (202) 366-1407.

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

Agency Comments and OIG Response

On August 14, 2019, CLA provided DOT with its draft report and received DOT's response on September 16, 2019. DOT's response is included in its entirety in the attached independent auditor's report.

DOT concurs with recommendation 10 and has provided appropriate actions and completion dates. Accordingly, CLA considers recommendation 10 resolved but open pending completion of the planned actions.

DOT partially concurs with recommendations 1, 2, 4, 8, 9, 11, and 12. The Department's proposed alternative actions meet the intent of CLA's recommendations. Therefore, CLA considers recommendations 1, 2, 4, 8, 9, 11, and 12 resolved but open pending completion of planned actions.

DOT partially concurs with recommendations 3, 5, 6, 7, 13 and 14. The Department's proposed alternative actions do not meet the intent of CLA's recommendations. Therefore, CLA considers these recommendations open and unresolved, and requests that DOT reconsider its positions on recommendations 3, 7, 13, and 14, and provide detailed responses for recommendations 5 and 6.

DOT partially concurs with recommendation 3, and proposes an alternative action to work with applicable OA representatives to review assessment and authorization processes, and implement a process to ensure that updated security plans, ATOs, and risk assessments are reviewed and updated to reflect applicable system controls, and technical vulnerabilities, and that current risks are clearly presented to the authorizing officials. DOT will also require the Federal Aviation Administration to ensure the same for its systems. DOT plans to complete this action by April 6, 2020. However, these planned actions will not meet the intent of CLA's recommendation because they do not address the inclusion of privacy controls in system security plans. While privacy related documentation such as PIAs may contain privacy controls, they do not address all privacy controls described in the National Institute of Standards and Technology Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations."* Therefore, CLA considers its recommendation 3 open and unresolved, and requests that the Agency reconsider its position.

DOT partially concurs with recommendations 5 and 6, and indicates that the intent of these recommendations is already addressed by existing policies. However, DOT has not demonstrated how these policies—provided to CLA after the draft report was issued—address the recommendations. Most importantly, CLA identified systems with significant security weaknesses across the common

operating environment, including unsupported operating systems subject to known compromises without adequate security mitigations. Therefore, CLA considers its recommendations 5 and 6 open and unresolved until CLA receives DOT's detailed response.

DOT partially concurs with recommendation 7, and states that this recommendation is a duplication of recommendation 15 from the FISMA 2014 audit regarding identity and access management. However, the prior-year recommendation 15 was specifically related to personal identity verification. Therefore, DOT's proposed actions do not meet the intent of recommendation 7 because they do not address weaknesses in identity and access management, including but not limited to overall access control policies and procedures, account management controls, remote access, and rules of behavior. CLA considers its recommendation 7 open and unresolved, and requests that the Agency reconsider its position.

DOT partially concurs with recommendation 13, and proposes an alternative action to ensure that the DOT COOP incorporates additional context and information regarding departmental information system contingency plans. This response does not address the intent of CLA's recommendation to review and update the COOP. During the audit, an updated version of the COOP was not provided to CLA for evaluation to demonstrate evidence of annual review within a history or revision log. DOT's response does not meet the intent of CLA's recommendation because it does not ensure COOPs are reviewed and updated on an annual basis. Therefore, CLA considers its recommendation 13 open and unresolved, and requests that the Agency reconsider its position.

DOT partially concurs with recommendation 14, and proposes an alternative action to ensure the DOT COOP provides additional context on the link between organizational BIAs and system-level BIAs, and that documentation is updated appropriately. DOT plans to complete this action by October 2, 2020. However, this response does not meet the intent of CLA's recommendation because it does not address actions to ensure contingency plans are complete, reviewed timely, approved, and tested. Therefore, CLA considers its recommendation 14 open and unresolved, and requests that the Agency reconsider its position.

Actions Required

We consider recommendations 1, 2, 4, 8, 9, 10, 11, and 12 resolved but open pending completion of planned actions. We consider recommendations 3, 5, 6, 7, 13, and 14 open and unresolved due to the Department's planned mitigating actions that do not address the intent of CLA's recommendations. CLA requests

the Department reconsider its position and provide OIG with a revised response within 30 days of the date of this report in accordance with DOT Order 8000.1C.

Exhibit. List of Acronyms

ATO	authorization to operate
BIA	business impact assessment
CIO	Chief Information Officer
CLA	CliftonLarsonAllen, LLP
COOP	continuity of operations plan
DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of the Secretary of Transportation
POA&M	plan of action and milestones
PIA	privacy impact assessment
QCR	quality control review

Attachment. Independent Auditor's Report

U.S. Department of Transportation's 2019 Federal Information Security Modernization Act (FISMA) Audit

October 8, 2019

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

October 8, 2019

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

Dear Mr. King:

CliftonLarsonAllen LLP (CLA) is pleased to present our performance audit report on the U.S. Department of Transportation's (DOT) information security management program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Federal Information Security Modernization Act of 2014 (FISMA) for the twelve months ending on June 30, 2019.

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

Very truly yours,

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Assistant Inspector General for Financial and Information Technology Audits
U.S. Department of Transportation
Office of Inspector General

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the U.S. Department of Transportation's (DOT) information security management program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and with the Federal Information Security Modernization Act of 2014 (FISMA or Act) for the fiscal year 2019. FISMA requires agencies to develop, implement, and document an Agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual review of their agencies' information security programs and report the results to the Office of the Management and Budget (OMB).

For the fiscal year 2019, OMB required IGs to assess 67 metrics in five security function areas – Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' information security programs and the maturity level of each function area. The maturity levels range—from lowest to highest—Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Consistent with FISMA and OMB requirements, our audit objective was to determine the effectiveness of DOT's information security program and practices in five function areas – Identify, Protect, Detect, Respond and Recover – for the 12 months ending on June 30, 2019.

Our audit was performed in accordance with the performance audit standards specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

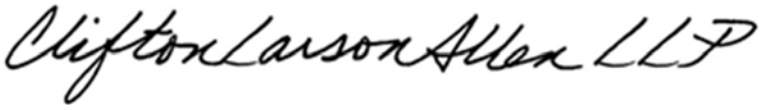
To address OMB's 2019 FISMA reporting metrics, we reviewed select controls for a sample of 64 DOT FISMA reportable systems, performed a vulnerability assessment and penetration test, interviewed Department officials, and reviewed data such as system security documentation. Refer to Appendix A for details on our scope and methodology. We also reviewed 42 of the OIG prior year open recommendations related to DOT's security program and practices. Appendix B contains the details of the prior year recommendations. Appendix C lists the organizations we visited or contacted.

Based upon our audit of DOT's information security program and practices, we concluded that in all five function areas, DOT is at the Defined maturity level – the second lowest level in the maturity model for an information security program, and thus not effective. The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT still faces significant challenges in the consistent implementation of its information security program across the Department. Consequently, we noted weaknesses in each of the eight Inspector General FISMA Metric Domains encompassing the Department's Agency-wide program. The audit identified continuing deficiencies related to risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training,

information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

We made 14 new recommendations to help the Department address challenges in its development of a mature and effective information security program. DOT concurs with one of our recommendations and partially concurs with thirteen of our recommendations. Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP



Arlington, Virginia
October 8, 2019

Table of Contents

Executive Summary

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

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

FISMA requires us to assess the maturity of five functional areas in DOT's information security program[3] and practices. This assessment used objective metrics that are standardized across the Federal government. To be considered effective, an Agency's information security program must be rated *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5).

DOT's overall information security program and the effectiveness of its security program and practices in accordance with Generally Accepted Government Auditing Standards (GAGAS) and FISMA did not meet the requirements to be considered effective. Based upon our audit of DOT's information security program and practices, we concluded that in all five function areas, DOT is at the Defined maturity level – the second lowest level in the maturity model for an information security program, and thus not effective. All five functional areas at DOT achieved a maturity level of Defined (Level 2). The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT faces significant challenges in the consistent implementation of its information security program across the Department.

Specifically, this audit identified continuing deficiencies related to risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

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

[2] The fiscal year (FY) 2019 metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover.

[3] The FY 2019 metrics are based on a maturity model approach begun in prior years and align the metrics with all five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover.

To address these weaknesses, we made 14 new recommendations to help the Department address challenges in its development of a mature and effective information security program. In addition, our review of prior FISMA recommendations, determined that 42 of the OIG prior year open recommendations related to DOT's security program and practices remain open.[4]

[4] Refer to Appendix B for a list of open recommendations from the OIG's prior FISMA audits.

Background

DOT Overview

The top priorities at DOT are to keep the traveling public safe and secure, increase their mobility, and have a transportation system contributing to the nation's economic growth. DOT employs almost 55,000 people across the country, in the Office of the Secretary of Transportation (OST) and its Operating Administrations (OAs) and bureaus, each with its own management and organizational structure. An Agency's information security program is considered effective once it achieves a rating of Level 4, *Managed and Measurable*. For DOT, secure information helps protect both taxpayers' dollars and citizens' safety since many of its systems support transportation related operations including air traffic control and pilot licensing. Others support inspection and oversight for highway safety and hazardous material transport.

The DOT's eleven OAs, manage the Department's 467 information technology (IT) systems.[5] The Department relies on these systems to carry out its missions, including safe air traffic control operations, qualified commercial drivers, and safe vehicles. DOT must also ensure the integrity of data in reports that account for billions of dollars used for major transportation projects such as highway construction and high-speed rail development. DOT's cybersecurity program is critical to protect these systems from malicious attacks or other compromises that may inhibit its ability to carry out its functions and missions.

DOT's operations rely on 467 IT systems, 328 (70%) of which belong to the Federal Aviation Administration (FAA). These systems represent an annual investment of approximately $3.5 billion – one of the largest IT investments among Federal civilian agencies. Moreover, the Department's financial IT systems are used to award, disburse, and manage approximately $99 billion in Federal funds annually.

FISMA Legislation

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

The Act also provides a mechanism for improved oversight of Federal Agency information security programs. FISMA requires Agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) a security incident response capability is established, and (3) information security management processes are integrated with the Agency's strategic and operational planning processes. All agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program.

[5] DOT's population of systems includes 467 systems as of April 3, 2019. For the purposes of this audit and our sample system selection, we excluded all systems that have an operational status of "Implementation" as these systems are still in development. Additionally, we excluded all systems included in the population that had the "FISMA Reportable" field marked as false or had a response in the "Type" field other than "Major Application" or "General Support System." This resulted in a population of 435 systems.

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

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

FY 2019 IG FISMA Reporting Metrics

OMB and Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. Accordingly, the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[6]

The FY 2019 metrics are based on a maturity model approach begun in prior years and align the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 1**.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 2** explains the five maturity model levels.

[6] https://www.dhs.gov/publication/fy19-fisma-documents.

A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

Table 2: IG Evaluation Maturity Levels

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

Summary of Results

DOT's overall information security program and the effectiveness of its security program and practices in accordance with GAGAS and FISMA did not meet the requirements to be considered effective. Overall and in each of the five function areas, DOT remains at the Defined maturity level. The Department has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT faces significant challenges in the consistent implementation of its information security program across the Department. In addition, controls need to be applied in a holistic manner to information systems across DOT in order to be considered consistent and fully effective by achieving at least a rating of Level 4, *Managed and Measurable*.

Current Results

DOT must make additional improvements to achieve an effective information security program. Specifically, this audit identified continuing deficiencies related to risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

Our conclusions as to the effectiveness of DOT's IT security program and practices incorporate multiple sets of test results, and are set forth below.

1. FISMA Maturity Levels

FISMA requires evaluators across the Federal government to respond to 67 objective questions, from which a DHS algorithm calculates a maturity score for each of the five functional areas. As set forth in the chart below, DOT was rated at *Defined* (Level 2) in each of the five functional areas.[7] However, by these objective metrics, DOT's overall security program fell below the minimum specified threshold of effective, which is Level 4, *Managed and Measurable*. **Table 3** below summarizes the maturity ratings and assessment by function.

Table 3: FY 2019 IG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions[8]	Metric Domains	Maturity Level	Cyberscope Evaluation
Identify	**Risk Management**	Defined (Level 2)	Not Effective
Protect	**Configuration Management**	Defined (Level 2)	Not Effective
	Identity and Access Management	Defined (Level 2)	Not Effective

[7] The most frequent maturity level rating across the Protect function served as the overall Protect function rating.
[8] See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

Cybersecurity Framework Security Functions[8]	Metric Domains	Maturity Level	Cyberscope Evaluation
Protect	**Data Protection and Privacy**	Defined (Level 2)	Not Effective
	Security Training	Defined (Level 2)	Not Effective
Detect	**Information Security Continuous Monitoring**	Defined (Level 2)	Not Effective
Respond	**Incident Response**	Defined (Level 2)	Not Effective
Recover	**Contingency Planning**	Defined (Level 2)	Not Effective
Overall	**Not Effective**		

2. Detailed Findings

Although DOT has, for the most part, formalized and documented its policies and procedures, and strategies, DOT continues to face significant challenges in its consistent implementation of its information security program. DOT has not made progress in addressing the security weaknesses noted in prior years, with work still remaining to continue correcting these deficiencies. In addition, controls need to be applied in a holistic manner to information systems across DOT in order to be considered consistent and fully effective. In this year's audit, we identified areas in the information security program that require strengthening. **Table 4** below summarizes our detailed findings.

Table 4: Cybersecurity Framework Security Functions mapped to weaknesses noted in FY 2019 FISMA Audit

FY 2019 IG FISMA Metric Domains	Weaknesses Noted in 2019
Risk Management	The policies, procedures, and documentation included in the DOT enterprise risk management program were not consistently implemented or applied across all DOT systems.
	Plans of Actions and Milestones (POA&Ms) and information security weaknesses were not effectively managed.
	Security Assessment and Authorization (SA&A) documentation were not properly approved, controls were not tested or clearly scheduled for testing, or security documentation were outdated or did not exist.

FY 2019 IG FISMA Metric Domains	Weaknesses Noted in 2019
	The system inventory maintained in Cybersecurity Assessment and Management System (CSAM) was not accurate.
	System hardware inventories were unable to be reconciled.
	Risk management policy and procedure documentation was not consistently maintained.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Unresolved configuration management weaknesses related to policies and procedures, vulnerability management, and configuration weaknesses.
Identity and Access Management	Unresolved user identity and access management weaknesses in access control policies and procedures, account management controls, remote access and rules of behavior.
	Incomplete deployment of two-factor user authentication mechanisms.
Data Protection and Privacy	Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs) and System of Records Notices (SORNS) were either not completed or updated.
Security Training	Specialized security training requirements were inconsistent and not fully implemented.
Information Security Continuous Monitoring	Performance metrics were not developed or utilized to measure the effectiveness of DOT's information system continuous monitoring program.
Incident Response	Incident response plans were not developed for all OA's.
	Incidents were not resolved in a timely manner.
Contingency Planning	Business Impact Analysis (BIAs) were inconsistently utilized for all systems.
	Contingency plans were either out of date, incomplete or missing for some systems.
	Contingency plans were not tested in a timely manner for some systems.

At present, the weaknesses that we identified leave DOT operations and assets at risk of unauthorized access, misuse and disruption. To address these weaknesses, we made 14 new recommendations to help the Department address challenges in its development of a mature and effective information security program. In addition, based on our follow-up on prior year recommendations, we determined that 42 of the OIG prior year open recommendations related to DOT's information security program and practices remain open. See Appendix B for a list of open recommendations from the OIG's last eight FISMA audits.

The following section provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions. Appendix A describes the audit scope and

methodology. Appendix B describes the current status of open recommendations from prior FISMA reports. Appendix C provides a listing of the organizations visited or contacted. Appendix D provides a listing of the representative subset of sampled systems. Appendix E contains management comments to the report.

FISMA Audit Findings

Security Function: Identify

Overview

DOT developed and published the DOT Cybersecurity Compendium to describe its entity-wide information security risk management program and Risk Management Framework (RMF). The RMF addresses both security and privacy controls. DOT's IT risk management process focused on identifying and evaluating the threats and vulnerabilities to DOT information. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. However, DOT' risk management process still requires time to mature to be an effective continuous monitoring tool since gaps and inconsistent implementation of the policies and procedures continue to exist.

Metric Domain – Risk Management

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

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

We also identified system inventory weaknesses, including OA system inventory listings not consistently aligning with the Department system inventory in the CSAM.[9] In addition, hardware inventory data reported within the Office of Chief Information Officer (OCIO) FISMA Metrics was not supported by artifacts provided by the OAs. Further, three OAs had not developed their own risk assessment policies and procedures.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* is guidance for implementing risk management framework controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The goal of the RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

[9] The Department's main repository to track system inventories, security assessment and authorization documentation, weaknesses, and other system security information.

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

Plans of Actions and Milestones

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

However, we noted that POA&Ms were not effectively managed throughout the Department. According to DOT's central reporting database, CSAM, the Department had approximately 10,499 open POA&Ms as of June 30, 2019, as compared with 9,793[10] open POA&Ms in FY 2018. Of the total number of open POA&Ms in 2019, 9,760 or 93 percent are under the FAA. This large number of open POA&Ms for FAA reflects ongoing efforts to migrate, integrate, and reconcile FAA security control weaknesses into CSAM from another system.

In addition, for the sample of DOT systems, we identified deficiencies in security weakness management related to the reporting, managing and closing of POA&Ms. Specifically, we identified: (a) POA&Ms not consistently established or updated to consider all known security weaknesses; (b) action items which missed major milestone dates and not updated to accurately reflect their current status; (c) POA&Ms which were missing attributes and details, such as cost requirements; and (d) POA&Ms which lacked sufficient documentation to justify closure. OCIO did not enforce requirements for ensuring the monitoring and timely remediation of weaknesses.

Specifically, we identified the following POA&M weaknesses for the sample of systems:

- 35 of 64 sampled systems, or 54.7 percent, POA&Ms were not consistently established for controls that were identified as non-compliant during Security Control Assessments (SCAs). Based on our sample, we estimate that 265 of 435 systems,[11] or 60.9 percent,[12] [13] have not established POA&Ms for controls that were identified as non-compliant during SCAs.
- 37 of 64 sample systems, or 57.8 percent, POA&Ms were not consistently established for controls that were listed as not in place in System Security Plans (SSPs). Based on our sample, we estimate that 254 of 435 systems, or 58.5 percent,[14] have not established POA&Ms for controls that were listed as not in place in SSPs.
- 34 of 64 sampled systems, or 54.7 percent, open POA&Ms either missed scheduled completion dates without updates or justifications, or were established with missing attributes and details such as cost requirements. Based on our sample, we estimate that 261 of 435 systems, or 60.1 percent,[15] have POA&Ms that have either missed scheduled

[10] *FISMA 2018: DOT's Information Security Program and Practices* (DOT OIG Report Number FI-2019-023, 3/20/2019).

[11] DOT's population of systems includes 467 systems as of April 3, 2019. For the purposes of our sample, we excluded all systems that have an operational status of "Implementation" as these systems are still in development. This resulted in a population of 435 systems.

[12] Our 60.9 percent estimate has a margin of error of +/- 9.8 percentage points at the 90 percent confidence level.

[13] Extrapolated rates are not equal to the simple ratio of errors found out of 64 sampled systems/risk-level combinations, since the extrapolation takes into consideration the stratified nature of the sampling design.

[14] Our 58.5 percent estimate has a margin of error of +/- 9.9 percentage points at the 90 percent confidence level.

[15] Our 60.1 percent estimate has a margin of error of +/- 9.9 percentage points at the 90 percent confidence level.

completion dates without updates or justifications, or were established with missing attributes and details such as cost requirements.
- 19 of 64 sample systems, or 29.7 percent, POA&Ms were closed without sufficient justification or evidence to support the remediation of the weakness. Based on our sample, we estimate 125 of 435 systems, or 28.7 percent,[16] have POA&Ms that were closed without sufficient justification or evidence to support the remediation of the weakness.

DOT Policy[17] requires each POA&M item to be completed with DOT mandatory fields including but not limited to: status, estimated cost, scheduled and actual completion dates, milestones, and milestone changes. Management did not ensure DOT policy was followed for the management of POA&Ms.

In addition, although FISMA audit recommendations are maintained by the Chief Information Security Officer (CISO) within a spreadsheet, these security control weaknesses were not being tracked and monitored within the official repository tool for IT weakness tracking and reporting as POA&Ms. Thus, weakness remediation efforts and current status from a tracking, visibility and oversight perspective of these weaknesses were not being properly captured and reported.

Incomplete information on POA&Ms in CSAM inhibits the CIO's and CISO's abilities to assess risk and funding requirements, analyze weakness trends, and implement department-wide solutions. In addition, without properly managing POA&Ms, DOT is at risk of operating systems and applications with known security weaknesses that are not being adequately tracked or remediated.

Security Assessment and Authorizations

Security Assessment and Authorization (SA&A) documentation was not effectively managed throughout the Department. As a result of system owners not effectively managing their systems and complying with DOT policies, for the sample of DOT systems within scope across the OAs, we noted weaknesses related to the creation, maintenance, monitoring, and retention of SA&A documentation. Departmental policy[18] requires OAs to annually assess security controls for their information systems and operating environments, and examine the following security documentation: system security plan, security assessment report and security assessment plan.

However, we noted the following weaknesses related to SA&A processes:

- For 15 of the 64 sample systems, or 23.4 percent, the Authorization to Operate (ATO) was either not signed, or not authorized by the appropriate Authorizing Official. Based on our sample, we estimate 116 of 435 systems, or 26.7 percent,[19] have an ATO that is either not signed or not authorized by the appropriate Authorizing Official.
- For 49 of 64 sample systems, or 76.6 percent, System Security Plans (SSPs) did not include all baseline security and privacy controls, were not current or updated annually, did not include updated implementation statements, or were not provided. Based on our sample, we estimate 345 of 435 systems, or 79.3 percent,[20] have SSPs that did not include

[16] Our 28.7 percent estimate has a margin of error of +/- 9.4 percentage points at the 90 percent confidence level.

[17] DOT *Cybersecurity Compendium Supplement to DOT Order 1351.37 v4.2,* May 2018.

[18] DOT CA-2, *DOT Cybersecurity Compendium*, 2018.

[19] Our 26.7 percent estimate has a margin of error of +/- 8.9 percentage points at the 90 percent confidence level.

[20] Our 79.3 percent estimate has a margin of error of +/- 8.2 percentage points at the 90 percent confidence level.

all baseline security and privacy controls, were not current or updated annually, did not include updated implementation statements, or could not be provided.
- For 24 of 64 sample systems, or 37.5 percent, SCAs were not performed annually, or not provided. Based on our sample, we estimate 174 of 435 systems, or 40.1 percent,[21] did not perform SCAs annually or could not provide evidence a SCA was completed.

In addition, we identified the following regarding Information Security Continuous Monitoring (ISCM) and Security Assessment Reports (SARs):

- For 58 of 64 systems, or 91 percent, the ISCM Plans did not include a current control assessment schedule, did not include all baseline and privacy controls, did not include a plan and were only an assessment schedule, were not current or expired, or were not provided.
- For 49 of 64 sample systems, Risk Assessments (as documented within a SAR) did not include environmental risks, did not include the likelihood, impact, and mitigation, were not current or expired, or were not provided.

Without assessing the effectiveness of security controls on a continuous basis, DOT does not have assurance that controls are operating effectively and this may expose the Department to information loss, fraud, or abuse. In addition, the lack of adequate security plans, assessments and/or continuous monitoring, makes it difficult for authorizing officials to make effective decisions regarding the risk for compromise created by system operation.

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.[22] However, we identified information systems which were listed in CSAM (the official system of record for DOT system inventory), which were not within system inventory listings maintained by the OAs, or information systems which were identified as operational by the OAs, however, not listed within CSAM. For example, one National Highway Traffic Safety Administration (NHTSA) system, and one OST system were noted in the CSAM inventory but were not in the respective OA system inventories. In addition, one NHTSA system was reported within CSAM on 4/3/19 as a FISMA reportable Major Application in Operational Status and was selected as system in scope of FISMA audit; however, the system ATO had expired in November 2018 and a decision was made in 2018 to change the operational status to "Retired." CSAM was not updated to reflect this change in operational status until April 2019.

The Department CISO indicated that the CSAM inventory is the official system inventory for the Agency; however, the OAs are also maintaining inventories outside of CSAM that are not reconciled to the Department system inventory. The absence of a complete and accurate inventory of all information systems, creates a risk that the Department may not identify and address all existing vulnerabilities.

[21] Our 40.1 percent estimate has a margin of error of +/- 10.2 percentage points at the 90 percent confidence level.

[22] DOT's *FISMA Inventory Guide*, Version 1.1, dated September 2013.

Asset Inventory

NIST standards[23] require DOT to develop and document a comprehensive inventory of information system components that accurately reflects the current information systems, includes all components within the authorization boundary of the system and is at the level of granularity deemed necessary for tracking and reporting. OAs are required to provide quarterly updates to OCIO on the current inventory for overall reporting to OMB.

However, OCIO has not provided the OAs with clear guidance on reporting of asset inventories. This lack of guidance has resulted in inconsistencies in the information that OCIO and OAs report. Specifically, we identified hardware inventory information reported within the OCIO FISMA Metrics that was not clearly supported by artifacts provided. From our analysis of 10 OAs' hardware asset inventories, approximately 70,889 assets were accounted for out of the 103,703 total assets reported in the FY 2019 Quarter 2 OCIO FISMA Metrics. This leaves a total of 32,814 assets not properly accounted for. Of the assets not accounted for, there were 16,659 mobile devices, 2,630 servers, and 13,545 workstations. In addition, OA's did not provide workstation listings for four OAs (FTA, MARAD, OIG, and PHMSA), server listings for two OAs (MARAD and OIG), and mobile device listings for all OAs.

DOT may not be aware of all assets residing in their environment and therefore may not be appropriately managing and protecting all assets.

Risk Assessment Policies and Procedures

We identified three OAs (MARAD, NHTSA and OST) who had not developed their own risk assessment policies and procedures, as they indicated they followed the Department policy. However, the DOT's Cybersecurity Compendium[24] states that each OA must develop, disseminate, review and annually update risk management policies and procedures that include appropriate elements such as criteria for making risk based decisions. The lack of policies which address how OAs assess risks, could expose the Department's information systems to compromise.

Without effective risk management controls, DOT is at risk of controls not operating as intended or not being implemented, increasing the likelihood of unauthorized modification, loss, and disclosure of critical and sensitive DOT information.

Recommendations:
We recommend that the DOT Chief Information Officer take the following actions in addition to the prior open recommendations[25] related to the weaknesses noted for the Identify function:

1. Perform a review of all POA&M items closed during the audit period to include supporting documentation and re-approve their closure.

[23] NIST Special Publication SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015 – security control, CM-8 Information System Component Inventory.

[24] *Departmental Cybersecurity Compendium: Supplement to DOT Order 1351.37 Departmental Cybersecurity Policy*, 2018.

[25] Prior FISMA open recommendations related to the findings noted within the "Identify" function: Rec. 9, (DOT OIG Report # FI-2016-001, 11/5/2015); Recs. 2, 5, 6, (DOT OIG Report # FI-2017-008, 11/16/2016); Rec. 3, (DOT OIG Report Number FI-2019-023, 3/20/2019); Rec. 9, (DOT OIG Report Number FI-2019-023, 3/20/2019); and Rec. 1, (DOT OIG Report # FI-2018-017, 1/24/2018). These recommendation are not being repeated within this report.

2. Revise current security weakness management policies and procedures (documenting within a revision history table) to require documented evidence such as calendar appointments, meeting minutes, etc. in support of POA&M closure decisions to be uploaded into CSAM.

3. Work with the OA CIOs to review current assessment and authorization processes and implement a validation process to ensure updated security plans, ATOs and risk assessments are reviewed and updated to reflect all system (including privacy) controls, vulnerabilities, and that current risks are clearly presented to the authorizing officials.

4. Work with the OA CIOs to develop mechanisms to ensure updated system security plans and assessments of security controls (that were previously assessed as not satisfied or partially satisfied) reflect current operational environments, including an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.

Security Function: Protect

Overview

DOT's Protect controls which cover configuration management, identity and access management, data protection and privacy, and security training were not effective and not consistently implemented across the Department. In FY 2019, DOT continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. However, controls require cycle time and institutional maturity to be consistently implemented across systems to resolve the security weaknesses. Weaknesses in the DOT IT environment continue to contribute to deficiencies in system configuration, data protection and privacy, access controls, and security training.

Metric Domain – Configuration Management
To secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. Furthermore, NIST has developed a repository of secure baselines for a wide variety of operating systems and devices.

OCIO does not enforce OMB's requirements[26] for addressing weaknesses in configuration management. We identified deficiencies in configuration management controls, designed to ensure DOT's critical systems have appropriate security baselines, current and vendor supported operating systems, accurate system and software inventories and up-to-date vulnerability patches. DOT policy[27] provides policies on mandatory configuration settings for information technology hardware, software and firmware. However, during our testing, we identified unsupported operating systems, unsupported software, and inadequate network segmentation, which could permit other systems to be exposed to weaknesses noted in the Common Operating Environment (COE). In addition, DOT Microsoft Windows servers had inconsistent baseline configurations.

Independent vulnerability and penetration testing assessments of DOT's COE and a sample of systems identified critical and high risk vulnerabilities related to patch management, configuration management, and unsupported software that may allow unauthorized access into mission-critical systems and data. Due to the vulnerabilities identified, the assessment team was able to successfully exploit certain vulnerabilities.

DOT has not consistently implemented the vulnerability remediation and management process. Unsupported operating systems, unpatched applications and configuration weaknesses existed without adequate protection. In addition, DOT has not clearly mapped assets as correlated to the OAs in the COE and the COE has limited segmentation between vulnerable hosts.

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

[26] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (2013).
[27] *DOT Security Weakness Management Guide,* March 2018.

Further, our analysis of POA&Ms for the sample of 64 systems in scope, noted configuration management control weaknesses related to (including but not limited to): policies and procedures, baseline configurations, change management controls, security impact analysis, and configuration settings, which were overdue for completion. A large number of the past due POA&Ms belonged to FAA. OCIO did not enforce requirements for addressing configuration management weaknesses and for ensuring the monitoring and timely remediation of weaknesses.

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

Metric Domain – Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized to access information and information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, and the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. Homeland Security Presidential Directive 12 calls for all Federal departments to require personnel to use personal identity verification cards. This use of personal identity verification cards is a major component of a secure, government-wide account and identity management system.

OMB required that, by 2012, all Federal employees and contractors use personal identity verification (PIV) cards to log into Agency computers and system applications. The use of PIV cards is part of multifactor authentication, which requires a system user to authenticate his or her identity by at least two unique factors. The DOT Cybersecurity Compendium, section DOT-IA.2.b, requires information systems to use the DOT Public Key Infrastructure (PKI) (as implemented through the use of PIV cards) assigned to DOT personnel as the system's primary authentication mechanism in support of multifactor authentication, at both the system and application level, for authentication of DOT employees and contractors.

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

We noted the following information security weaknesses in the identity and access management domain:

- The Department has not transitioned 222 systems to be enabled to use PIV (or another form of two-factor authentication or an authentication mechanism was unspecified).
- 56 systems were PIV enabled; however, PIV was not enforced as the primary authentication method.
- 92 of 202 systems which contain Personally Identifiable Information (PII) did not require PIV authentication.
- We found weaknesses (POA&Ms) related to user identity and access management in 21 of 41 sampled FAA systems that had passed or were approaching their remediation dates. Additionally, we noted weaknesses in user identity and access management for 1 of 23

sampled Non-FAA systems that had passed their remediation dates, and 3 of 23 sample systems had open POA&Ms. These weaknesses were related to the following access management areas (included but not limited to): overall access control policies and procedures, account management controls, remote access, and rules of behavior.

OCIO did not enforce requirements for addressing access and identity management weaknesses and for ensuring the monitoring and timely remediation of weaknesses. Control weaknesses in identity and access management may expose DOT to increased risk of data compromise and may lead to unauthorized access to DOT's information systems.

Metric Domain – Data Protection and Privacy

FISMA requires the Federal government to establish a privacy program and corresponding policies and procedures for the protection of PII collected, used, maintained, shared, and disposed of by information systems. Training is to be provided for personnel responsible for PII or activities involving PII. Documentation to be maintained as part of an effective privacy program include Privacy Impact Assessments (PIA), Privacy Threshold Assessments (PTAs) and System of Records Notices (SORN). In addition, agencies are required to develop a data breach response plan for reporting, investigating, and managing a privacy-related breach.

DOT Business Owners should be collaborating with System Owners to ensure all privacy regulatory compliance reporting changes are entered and updated as required in the CSAM system and/or any other DOT tracking system per the DOT Order 1351.18, *Privacy Risk Management*. Our review of the privacy inventory as provided by DOT, identified systems which were required to maintain relevant, current and accurate privacy data and artifacts, such as PTAs and PIAs. However, we noted that privacy data and artifacts for some DOT systems listed in the privacy inventory, were either not current or not developed for 38 out of 64 (59%) sampled systems. Additionally, the privacy inventory included 26 systems with PTAs which were last updated more than 3 years ago (5/12/16 or older), one system with a PTA date completed as To Be Determined (TBD), 13 systems containing PII with a PIA date completed of TBD, and 10 systems with PII and a SORN date completed of TBD.

Oversight of the Department's policies and procedures were not consistently implemented to ensure OAs were complying with documented policies. The majority of the Department's privacy risk derives from the collection, use, storage, and sharing of PII, and the IT systems used to support these processes. As a result, the lack of privacy protection puts the PII stored in DOT's information systems at risk for compromise.

Metric Domain – Security Training

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

Meeting security training goals decreases the possibility that employees will engage in activities that could lead to security compromises. Even though DOT met its security awareness training goals, the Department has conflicting policies and procedures (Department's Cybersecurity Compendium policy and Cybersecurity Action Memos (CAMs)) in regards to specialized training

requirements. Specifically, there are contradictory guidance and policies in regards to specialized training requirements in the area of positions subject to specialized training requirements, and how to measure whether training completed was sufficient (e.g. number of hours, or completion of specific courses which map to competency requirements). As a result, supervisors were responsible for identifying who required specialized training.

Although CAMs are issued to implement new cybersecurity requirements described within the Department's Cybersecurity Compendium policy, CAMs do not supersede the Compendium per the *Policy Order of Precedence Guidance* CAM.

Control weakness in the security training domain expose DOT to increased risk of unintentional and insecure user behavior in protecting the technology environment. Thus, DOT may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Recommendations:

We recommend that the DOT Chief Information Officer take the following actions in addition to the prior open recommendations[28] related to the weaknesses noted for the Protect function:

5. Document OA subnets and OA responsibilities for devices and systems operating on the Common Operating Environment.

6. Document and implement network segmentation to reduce the attack surface or susceptibility of vulnerable and sensitive OA assets in the Common Operating Environment.

7. Work with OAs to remediate outstanding identity and access management weaknesses through implementation and closure of POA&Ms and control assessments to determine whether these risks were addressed.

8. Work with Component Privacy Officers (POs) to develop and implement procedures then verify the completion, review, tracking and approval through review of updated PTAs, PIAs and SORNs.

[28] Prior FISMA open recommendations related to the findings noted within the "Protect" function: Rec. 9 (DOT OIG Report Number FI-2019-023, 3/20/2019); Rec. 6 (DOT OIG Report # FI-2018-017, 1/24/2018); Rec.15 (DOT OIG Report # FI-2015-009, 11/14/2014); Rec. 8, (DOT OIG Report # FI-2015-009, 11/14/2014); Rec. 7, (DOT OIG Report Number FI-2019-023, 3/20/2019). These recommendations are not being repeated within this report.

Security Function: Detect

Overview

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

Metric Domain – Information Security Continuous Monitoring

The goal of Information Security Continuous Monitoring (ISCM) is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

DOT continues to rely upon the metrics defined by the DHS to monitor the performance of their ISCM program, utilizing ISCM solutions such as ForeScout, IBM BigFix, Tenable Nessus, and Splunk to provide quantitative and qualitative measures, as documented within the DOT Guide.[29] However, from a review of dashboards from these ISCM solutions, it was not clear which specific quantitative and qualitative measures were being captured.

In addition, the quantitative and qualitative measures at the system level are predominately not defined. The only metric requirements that are defined, is for security awareness and specialized training. The OAs are required to capture quantitative and qualitative measures; however, the DOT ISCM strategy does not define what is being measured and the target level expected to be achieved.

Since DHS metrics are not tailored specifically for DOT's business environment, and DOT's Guide does not identify any process to develop such metrics, DOT is operating without properly developed DOT specific cybersecurity performance measures. The lack of these measures inhibits the Department's ability to monitor progress, identify areas that need attention and determine the effectiveness of its cybersecurity program, including ISCM. Additionally, artifacts which support the accuracy of hardware inventory counts reporting in CIO FISMA Metrics were not provided, and policies and procedures which describe how data (used to populate the CIO FISMA Metrics) is obtained, aggregated, validated and supported was not in effect during the audit period.

Without a Department defined requirement for the collection of qualitative and quantitative data, the analysis of the data will result in metrics that are not cohesive at the Department level. Therefore, the metrics may be incorrect and the risk of the DOT operating environment will be inaccurate. In addition, without properly collecting and analyzing qualitative and quantitative data to calculate metrics, DOT is at risk of operating systems and applications without awareness of the current operating environments. Further, without proper analysis of metrics, DOT cannot ensure that Risk Executives are properly informed of the operating environments and risks to their systems for authorization.

[29] *DOT Security Authorization & Continuous Monitoring Performance Guide*, January 2018.

Recommendations:

Prior FISMA recommendations[30] related to the weaknesses noted in the Detect function remain open and therefore, we are not making new recommendations.

[30] Prior FISMA open recommendations related to the findings noted within the "Detect" function: Recommendation 10, (DOT OIG Report Number FI-2019-023, 3/20/2019); Recommendation 2, (DOT OIG Report Number FI-2019-023, 3/20/2019); and Recommendations 1, 2 and 3 (DOT OIG Report Number FI2019014, 12/4/2018). These recommendations are not being repeated within this report.

Security Function: Respond

Overview

DOT did not follow its processes and procedures for handling incidents and therefore work remains to adequately measure and evaluate their incident response program and its effectiveness.

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

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

We noted the following information security weaknesses in DOT's incident response program.

- Based upon an examination of security incidents created during the audit period, we noted 47 incidents were still open and unresolved for over 90 days, with an average of 238 days unresolved, as of May 9, 2019, with 12 of these incidents related to proven or suspected PII compromises.

- The OCIO has an outdated Incident Response Plan (IRP). Specifically, the OCIO, *Cyber Security Incident Response Plan* (March 2014), requires a full review of the IRP to be completed annually to ensure its relevance and operational effectiveness. However, the Revision History and Approval table documents only the initial version and does not support annual reviews have been conducted. Additionally, there are references to the former incident ticketing system, Joint Advanced Solutions (JAS) system.

- The IRP for the OST OA was not updated in more than one year, and IRPs were not provided for the FMCSA, NHTSA, MARAD and FRA OA. The OAs (NHTSA, MARAD and FRA) had not developed an IRP at the OA level, since they relied upon the OCIO IRP. However, DOT Policy[31] requires OAs to provide component-specific incident handling procedures to the DOT CISO and DOT Computer Security Incident Response Center (CSIRC). The policy also requires that DOT Components with approved Component-

[31] *Departmental Cybersecurity Compendium*: Supplement to DOT Order 1351.37 D, Appendix A: DOT Department-wide NIST 800-53 Minimum Parameters, IR-1.e Incident Response Policy and Procedures.

specific incident handling procedures review and update them annually in accordance with DOT IR policy and procedures. Additionally, the OCIO, *Cyber Security Incident Response Plan*, 5.7 states, "Each OA will develop and coordinate respective incident management plans with the Cyber Security Operations Management Team and CSMC. For one OA (FMCSA) did not provide the IRP for the OA and the sampled OA systems as required by the FMCSA *Incident Response Guidelines Memorandum*, dated 3/28/17.

The process to close out incidents and to develop and to maintain updated incident procedures is not working as intended due to inadequate oversight. However, by not resolving and monitoring security incidents in a timely manner, there is an increased risk that DOT systems could be exposed to viruses and other malicious code, which could result in unauthorized access to mission critical systems and sensitive data. Also, there is an increased risk that security incidents may not be detected or resolved timely. In addition, without up-to-date incident response plans, there is an increased risk that security incidents may not be adequately recorded, tracked, investigated, or resolved and personnel may not be aware of responsibilities.

Recommendations:

We recommend that the DOT Chief Information Officer take the following actions:

9. Document and implement a process to ensure incident response procedures related to the timely notification, reporting, updating, and resolution of security incidents are followed in accordance with policy.

10. Review and update the OCIO *Cyber Security Incident Response Plan*, documenting evidence of review and revisions within a history log.

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.

Security Function: Recover

Overview

DOT has, for the most part, defined policies and procedures for developing, updating and testing its contingency plans; however, ongoing weaknesses remain in order to achieve control effectiveness and to ensure the program is consistently implemented across the Department.

Metric Domain – Contingency Planning

FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if loss of a system's availability occurs. Consideration of risk to an Agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods." Once a contingency plan is established, training and testing must be conducted to ensure that the plan and individuals tasked with the contingency responsibilities will be capable in the event of an emergency.

DOT has not consistently implemented contingency planning processes to reach a level of maturity as defined by Cyberscope metrics to be an effective overall program.[32] This is mainly because DOT's contingency plan program lacks a current Continuity of Operations (COOP) Plan, and for the sampled systems, we found contingency plans were either missing requiring elements, not reviewed, approved, or not updated in a timely manner, Business Impact Assessments (BIAs) were either incomplete, missing required information, or did not clearly define Recovery Time Objectives (RTOs) or Recovery Point Objectives (RPO), or contingency plans were not tested annually.

Specifically, the following information security weaknesses exist within the contingency planning domain:

- The DOT COOP Plan was not updated in a timely manner. The last revision/review to the COOP Plan was performed in June 2017.
- We found that seven OAs tested had not implemented DOT's contingency plans and testing requirements for at least one system. We also found systems not meeting OMB and FISMA requirements for contingency planning and testing. For example:
    - 33 of 64 sampled systems contingency plans were not updated timely, approved or missing required elements for some systems (FAA, FHWA, FRA, MARAD and PHMSA). Based on our sample, we estimate 237 of 435 systems, or 54.5 percent,[33] have contingency plans that have not been updated timely, have not been approved, or are missing required elements.

[32] A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

[33] Our 54.5 percent estimate has a margin of error of +/- 10 percentage points at the 90 percent confidence level.

- 13 of 64 sampled systems BIAs were not complete, missing required information, or did not clearly define RTO or RPO for some systems (FAA, FTA, MARAD, OST and PHMSA). Based on our sample, we estimate 71 of 435 systems, or 16.4 percent,[34] have BIAs that are not complete, missing required information, or did not clearly define RTOs or RPOs.
- Testing of contingency plans was not performed for 12 of 64 sampled systems in accordance with DOT requirements (FAA, FRA, MARAD and OST). Based on our sample, we estimate 76 of 435 systems, or 17.4 percent,[35] did not perform contingency plan testing in accordance with DOT requirements.

The process to review and update contingency plans, BIAs and perform contingency plan testing and performance of oversight of these activities is not effective.

Effective contingency planning and comprehensive testing is crucial to ensure departmental systems and data are available and IT systems and applications are resilient against outages and disruptions. Failure to consistently document Contingency Plans and recovery time objectives in BIAs, increases the risk that DOT will be inadequately prepared for system or service disruptions and outages. In addition, failure to comprehensively test and exercise documented plans increases the risk that weaknesses or areas of improvement would not be identified effectively in preparation for real-world contingency events.

Recommendations:

We recommend that the DOT Chief Information Officer take the following actions in addition to the prior open recommendations[36] related to the weaknesses noted for the Recover function:

13. Work with the OST's Office of Intelligence, Security and Emergency Response (S-60) to ensure the DOT COOP is reviewed and updated (noting evidence of the review within a history/revision log).

14. Work with the OA CIOs to remediate identified weaknesses in contingency plans and BIAs, such as missing information, lack of timely review, and inadequate approvals, demonstrated by updated contingency plans and BIAs.

[34] Our 16.4 percent estimate has a margin of error of +/- 7.6 percentage points at the 90 percent confidence level.

[35] Our 17.4 percent estimate has a margin of error of +/- 7.7 percentage points at the 90 percent confidence level.

[36] Prior FISMA open recommendations related to the findings noted within the "Recover" function: Recommendation 3, (DOT OIG Report # FI-2012-007, 11/14/2011) and Recommendation 12, (DOT OIG Report Number FI-2019-023, 3/20/2019). These recommendation are not being repeated within this report.

Conclusion

DOT relies on hundreds of information systems to carry out its missions, including safe air traffic control operations, and handling billions of dollars. DOT's cybersecurity program must protect these systems from malicious attacks and other compromises that may put citizen safety or taxpayer dollars at risk. While DOT continues to update its policies and procedures, and maintain a Defined level of maturity, we continue to find persistent deficiencies in the implementation of policies and processes that create an effective information security program. The effect of these deficiencies is exacerbated by the Department's growing "compliance" mindset and non-implementation of controls it believes are not required by law or regulation. These deficiencies place DOT's information systems at an increased risk of compromise and make them a target for malicious attackers.

Agency Comments and CLA Response

We provided DOT with our draft report on August 14, 2019, and received its response on September 16, 2019, which is included in its entirety as an appendix to this report. In its response, the Department notes that, for Fiscal Year 2019, they maintained an overall rating of "Managing Risk" under DHS's framework and risk management assessment methodology. While this is a positive result, it is important to note that DHS uses unaudited data submitted by the Department in order to determine its ratings. Additionally, this audit identified continuing deficiencies related to risk management, vulnerability and configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

DOT concurs with recommendation 10 as written. DOT states it plans to implement recommendation 10 by January 10, 2020.

DOT concurs in part with recommendation 1, and proposes an alternative action to develop and implement a risk-based oversight approach to review and assess the quality of closed POA&Ms from the last cycle (the audit period covered by this report) and update related policy, as appropriate. DOT plans to complete this action by September 8, 2020. DOT's proposed alternative actions meet the intent of recommendation 1. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 2, and proposes an alternative action to enhance implementation guidance regarding evidence for POA&M closure to include meeting minutes, and/or other appropriate documentation, without the inclusion of e-mail or calendar records. DOT plans to complete this action by April 6, 2020. DOT's proposed alternative actions meet the intent of recommendation 2. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 3, and proposes an alternative action to work with applicable OA representatives to review assessment and authorization processes and implement a process to ensure updated security plans, ATOs, and risk assessments are reviewed and updated to reflect applicable system controls, and technical vulnerabilities, and that current risks are clearly presented to the authorizing officials. DOT will also require the FAA to ensure the same for its systems. DOT plans to complete this action by April 6, 2020. However, these planned actions will not meet the intent of our recommendation, since they do not address the inclusion of privacy controls within system security plans. While privacy related documentation such as PIAs may contain privacy controls, they do not address all privacy controls described within NIST 800-53, Revision 4. Therefore, we consider our recommendation open and unresolved and request that the Agency reconsider its position.

DOT concurs in part with recommendation 4, and proposes an alternative action to ensure all applicable OA system security plans and assessments reflect the system architecture, and applicable security controls are properly evaluated. DOT will also require the FAA to ensure the same for its systems. DOT plans to complete this action by April 6, 2020. DOT's proposed alternative actions meet the intent of recommendation 4. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendations 5 and 6, and indicated that the intent of these recommendations are already addressed by existing policies. However, these policies were not provided during the period of audit despite numerous requests for this information. After the draft report was issued, these policies were provided. Additionally, DOT has not demonstrated how these policies and ongoing architecture and network management modernization efforts resulted in documented and implemented network segmentation actions to address the recommendations. Additionally, when the finding was presented to management initially, concurrence was received by DOT OCIO IT Shared Services (ITSS); however, subsequently overturned by the DOT CISO. The rationale was that the policies provided subsequent to the audit period addressed the recommendations. We identified systems with significant security weaknesses across the COE including unsupported operating systems subject to known compromises without adequate security mitigations, reporting on the state of the environment and systems scanned at a point in time. DOT stated it does not plan to address these recommendations because the intent of these recommendations is addressed by existing policy, and DOT requests closure within 30 days of the final report's issuance. Therefore, we consider these recommendations open and unresolved until we receive DOT's detailed response.

DOT concurs in part with recommendation 7, and states that this recommendation is a duplication of recommendation 15 from the FISMA 2014 audit regarding identity and access management. However, this statement is incorrect, as this prior year recommendation was referenced within the report as an open prior year recommendation within a footnote. The prior recommendation 15 was specifically related to the PIV finding and therefore, DOT's proposed actions do not meet the intent of our recommendation because they do not address weaknesses in identity and access management including but not limited to overall access control policies and procedures, account management controls, remote access, and rules of behavior as described within the finding. DOT's planned actions will not meet the intent of our recommendation to ensure outstanding identity and access management weaknesses are remediated. Therefore, we consider our recommendation open and unresolved and request that the Agency reconsider its position.

DOT concurs in part with recommendation 8, and proposes an alternative action to assess the capacity and capability of the Departmental and component level Privacy programs to implement required functions and processes and develop a corrective action plan based on the results of the assessment. Although DOT's response indicates that the CPO has established clear processes and guidance for the completion of privacy risk management activities, we noted various implementation issues such as expired PTAs and non-existent PIAs. DOT plans to complete this action by August 3, 2020. DOT's proposed alternative actions meet the intent of recommendation 8. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 9 and proposes an alternative action to update its processes to ensure the timely update and resolution of cybersecurity incidents. DOT plans to complete this action by August 3, 2020. DOT's proposed alternative actions meet the intent of recommendation 9. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 11, and proposes an alternative action to issue updated policy to clarify Component responsibilities for IT policies, including cybersecurity, and companion implementation guidance. DOT plan0s to complete this action by April 6, 2020. DOT's

proposed alternative actions meet the intent of recommendation 11. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 12, and proposes an alternative action to require that the FAA review its cybersecurity incident response plan on an annual basis and the Department will ensure that applicable Components are properly accounted for in a revised DOT enterprise-wide incident response plan. DOT plans to complete this action by April 6, 2020. DOT's proposed alternative actions meet the intent of recommendation 12. Therefore, we consider this recommendation resolved but open pending completion of planned actions.

DOT concurs in part with recommendation 13, and proposes an alternative action to ensure that the DOT COOP plan incorporates additional context and information regarding Departmental Information System Contingency Plans. This response does not address the intent of the recommendation to review and update the COOP plan. During our audit, an updated version of the COOP plan was not provided for our evaluation to demonstrate evidence of annual review within a history or revision log. However, this response does not meet the intent of our recommendation, as it does not address actions by DOT to ensure COOP plans are reviewed and updated on an annual basis. Therefore, we consider our recommendation open and unresolved and request that the Agency reconsider its position

DOT concurs in part with recommendation 14, and proposes an alternative action to ensure the DOT COOP plan provides additional context on the linkage between organizational business impact assessments (BIAs) and system-level BIAs, and that documentation is updated appropriately. DOT plans to complete this action by October 2, 2020. However, this response does not meet the intent of our recommendation, as it does not address actions to ensure contingency plans are complete, reviewed timely, approved and tested. Therefore, we consider our recommendation open and unresolved and request that the Agency reconsider its position.

Actions Required

We consider recommendations 1, 2, 4, 8, 9, 10, 11, and 12 resolved but open pending completion of planned actions.

We consider our recommendations 3, 5, 6, 7, 13 and 14 open and unresolved. We request that DOT reconsider its position and provide us with its revised response within 30 days of the date of this report in accordance with DOT Order 8000.1C.

Appendix A: Scope and Methodology

Scope

We conducted this audit in accordance with performance auditing standards, as specified in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Generally Accepted Government Auditing Standards (GAGAS) also require us to disclose impairments of independence or any appearance thereof. OMB requires that the FISMA template include information from all OAs, including OIG. OIG contracted with us to conduct the review of the DOT information security program and practices subject to our oversight. Although the OIG is a small component of the Department, based on number of systems, any testing pertaining to OIG or its systems does not impair our ability to conduct this mandated audit.

For this year's review, OMB required IGs to assess 67 metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security programs and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

Consistent with FISMA and OMB requirements, our audit objective was to conduct a performance audit of the DOT information security management program and practices in accordance with the GAGAS and with the FISMA in order to determine the effectiveness of DOT's information security program and practices in five function areas – Identify, Protect, Detect, Respond and Recover.

Our scope was to determine whether DOT implemented an effective information security program and practices for the 12-month period between July 1, 2018 and June 30, 2019, with a data collection cut-off date of June 30, 2019. The effectiveness of the information security program is defined as achieving a certain maturity level for each function area and domain based on the unique challenges of the organization.

For this audit, we reviewed select controls for a sample of 64 systems from a total population of 435 DOT FISMA reportable systems in operation.[37] They are broken down by the following number of systems by OA: FAA (41), OST (7), PHMSA (2), FHWA (2), FMCSA (2), FRA (2), FTA (2), MARAD (2), NHTSA (2) and OIG (2). One system was substituted for NHTSA, since it was determined the system was retired and subsumed into another system (refer to Appendix D for the specific systems).

We performed a vulnerability assessment and penetration testing covering the headquarters Common Operating Environment (COE), OST Facilities and Building Management System, Volpe Physical Access Control System and Airline Performance Economic Information System.

[37] We selected a stratified random sample from DOT's population of 435 FISMA Reportable Major Applications/General Support Systems noted as being in operation to assess the Agency's compliance with FISMA.

In addition, the audit included an assessment of effectiveness for each of the eight FY 2019 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions. The audit also included a follow up on prior audit recommendations to determine if DOT made progress in implementing the recommended improvements concerning its information security program and practices.

Audit fieldwork was performed at DOT's headquarters in Washington, D.C., during the period April 2019 through September 2019.

Methodology

To accomplish the audit objective, CLA:

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

DOT's population of systems includes 467 systems as of April 3, 2019. For the purposes of our sample, we excluded all systems that have an operational status of "Implementation" as these systems are still in development. Additionally, we excluded all systems included in the population that had the "FISMA Reportable" field marked as false or had a response in the "Type" field other than "Major Application" or "General Support System." This resulted in a population of 435 systems. We selected a stratified random sample from DOT's population of 435 FISMA Reportable Major Applications/General Support Systems noted as being in operation to assess whether the Agency's information security management program and practices were effective in accordance with the GAGAS and the FISMA.

The 435 systems were then divided into 14 strata based on the OA which the system belonged to and the FIPS 199 risk categorization. The sample size was calculated with two requirements:

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

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

extrapolated to the overall population based on well-established survey sampling theory.[38] The simulations were repeated 100 times, and the average estimates were obtained in this manner. We chose a sample size of 64 systems, which we estimated that it would result, on average, about a 10 percent margin of error.

In addition, CLA assessed DOT's technical controls by performing a network security test as part of the FISMA audit. The independent vulnerability assessment and penetration test was conducted to determine the effectiveness of internal controls that prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the vulnerability assessment and penetration test was incorporated into our FISMA audit results.

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

- OMB and DHS, FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.
- NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).

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

Appendix B: Open Recommendations from Prior FISMA Reports

The following is the status of open recommendations from prior FISMA reports. Current status of prior year FISMA open recommendations was determined through a review of the Department's overall status of prior recommendations and testing the effectiveness of DOT's information security program and practices covering the period July 1, 2018 through June 30. 2019. In addition, one closure package was reviewed related to one recommendation; however, the documentation provided was not sufficient to close the recommendation. Therefore, we determined that all prior year FISMA open recommendations (42) would remain open.

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

Prior Years' Open FISMA Recommendations as of June 30, 2019.

Fiscal Year 2010, OIG Report Number FI-2011-022	
Number	**Recommendation**
14	Identify and implement automated tools to better track contractors and training requirements.

Fiscal Year 2011, OIG Report Number FI-2012-007 *FISMA 2011: Persistent Weaknesses in DOT's Controls Challenge the Protection and Security of its Information System*	
Number	**Recommendation**
1	Enhance existing policy to address security awareness training for non-computer users, address security costs as part of capital planning, correct the definition of "government system", and address the identification, monitoring, tracking and validation of users and equipment that remotely access DOT networks and applications.
3	In conjunction with OA CIOs, create, complete or test contingency plans for deficient systems.

Fiscal Year 2013, OIG Report Number FI-2014-006	
Number	**Recommendation**
1	Obtain and review specialized training statistics and verify, as part of the compliance review process, that all employees with significant security responsibilities have completed the number of training hours required by policy. Report results to management and obtain evidence of corrective actions.
4	Obtain and review plans from FMCSA, MARAD, OST, and RITA to authorize systems with expired accreditations. Perform security reviews of unauthorized systems to determine if the enterprise is exposed to unacceptable risk.

7	Obtain a schedule and action plan for OAs to develop procedures for comprehensive cloud computing agreements to include security controls roles and responsibilities. Report to OA management any delays in completing the procedures.
8	Obtain and review existing cloud computing agreements to assess compliance with agency policy, including security requirements. Report exceptions to OA management.

Fiscal Year 2014, OIG Report Number FI-2015-009 *FISMA 2014: DOT Has Made Progress but Significant Weakness in Its Information Security Remain*	
Number	**Recommendation**
8	Work with the components to develop a plan to complete annual SAT training within plan milestones and improve tracking. Assess training periodically to determine if the component will meet SAT training plan.
15	Work with components to develop or revise their plans to effectively transition the remaining information systems to required PIV login. Create a POA&M with planned completion dates to monitor and track progress.
16	Work with the Director of DOT Security to develop or revise their plan to effectively transition the remaining facilities to required PIV cards.

Fiscal Year 2015, OIG Report Number FI-2016-001 *FISMA 2015: DOT has Major Success in PIV Implementation, But Problems Persist In Other Cybersecurity Areas*	
Number	**Recommendation**
1	The Deputy Secretary, or his designees, take action to ensure that the OCIO revises the Department's Cybersecurity policy to document exclusions for PIV required use for network and system access.
2	The Deputy Secretary, or his designees, takes action to work with the OAs to develop a formal transition plan to the proposed ISCM target architecture that includes but is not limited to: (1) continuously assessing security controls; (2) reviewing system configuration settings; and (3) assessing timely remediation of security weaknesses. During the transition period, establish processes and practices for effectively collecting, validating, and reporting ISCM data.
8	The Deputy Secretary, or his designees, takes action to work with FAA to improve their assessment process to meet DOT Cybersecurity Compendium and Security Authorization & Continuous Monitoring Performance Guide. DOT CIO in conjunction with the FAA CIO review the FAA quality assurance process to ensure all security documents are reviewed and updated to reflect the system controls, vulnerabilities, and that the current risks are clearly presented to the Approving Officials.
9	The Deputy Secretary, or his designees, takes action to work with the OAs to ensure they update open POA&Ms with the required data fields.

Fiscal Year 2016, OIG Report Number FI-2017-008 *FISMA 2016: DOT Continues to make progress, but the Department's information security posture is still not effective*	
Number	**Recommendation**
1	Work with all OAs to complete expired authorizations and reinforce or strengthen policy requiring systems be reauthorized prior to their expiration dates.
2	Work with all OAs to perform a thorough CSAM quality review to ensure system documentation matches what is entered into CSAM. At a minimum, the review should verify that: (1) system authorization dates in CSAM match what is approved by the authorizing official; (2) POAMs are created and reported once a security weakness is found; and (3) authorizing officials are provided accurate documentation on all risks accepted.
3	Work with FAA, FHWA, FMCSA, FTA, MARAD, NHTSA, and OST to develop risk acceptance memos for the expired systems identified in this report.
4	Work with OST COE, FTA, and FAA, the common control providers, to report and update risk acceptance for shared controls that are not implemented in DOT's Repository (e.g., CSAM) per FISMA, OMB, and DOT requirements.
5	Work with FAA and require them to review CSAM POA&M entries, and identify and correct cases where multiple weaknesses were entered as one.
6	Perform a review of CSAM POA&Ms and assess if the entries are compliant with DOT policy. For deficient data, require OAs to provide a corrective action plan.
7	Identify and document OST COE compensating controls when used to address security weaknesses in CSAM and system authorizations.
8	Report/update OST COE security weaknesses found during vulnerability assessments in DOT's Repository (e.g., CSAM) per FISMA, OMB, and DOT requirements.

Fiscal Year 2017, OIG Report Number FI-2018-017 *FISMA 2017: DOT's Information Security Posture is Still Not Effective*	
Number	**Recommendation**
1	Require MARAD, NHTSA, OST, and SLSDC to develop and disseminate policies and procedures for their risk management programs that include the appropriate elements such as criteria for making risk based decisions.
2	Implement controls to verify that information on threat activity has been communicated to senior agency officials and require retention of supporting documentation.

3	For the COE and FAA, update procedures and practices for monitoring and authorizing common security controls to (a) require supporting documentation for controls continual assessments, (b) complete reauthorization assessments for the controls, (c) finalize guidance for customers' use of controls, and (d) establish communication protocols between authorizing officials and common control providers regarding control status and risks.
4	Verify that FAA's criteria regarding designation and definition of contractor systems conforms to DOT guidance, and that systems are correctly classified.
5	Implement controls to continuously monitor and work with components to ensure network administrators are informed and action is taken to disable system accounts when users no longer require access or have been inactive beyond established thresholds.
6	Complete PIV enablement and requirements for remaining information systems, except those that are subject to exclusions that are documented and approved.
7	Take action to fully implement mandatory use of PIV cards for VDI access.
8	Implement processes verifying that personnel performing certain security related roles receive specialized training needed to meet OCIO guidance.

Fiscal Year 2018, OIG Report Number FI-2019-023 *DOT's Information Security Program and Practices*	
Number	**Recommendation**
1	Develop policy and procedures to verify and validate the accuracy and completeness of the Department's key FISMA information repository and tool, currently the Cyber Security Assessment and Management tool (CSAM).
2	Direct OCIO to follow policy and conduct annual cybersecurity performance analysis reviews of OAs' cybersecurity programs, and submit reports to OAs with recommendations to address cybersecurity weaknesses.
3	Develop a process and policy where applicable to ensure the Department develops and maintain a comprehensive and accurate inventory of cloud systems, contractor systems, and websites that the public can access.
4	Direct OST to prioritize and resolve COE security weaknesses identified by assessor, and develop POA&Ms that realistically reflect resources and timeframes for completions of these actions.
5	Direct OST to establish MOUs that delineate the responsibilities for COE common controls with each of the following OAs: FHWA, FMCSA, FRA, FTA, OIG, MARAD, SLSDC, and NHTSA.
6	Direct OAs (FAA, FHWA, FMCSA, FRA, FTA, OST, PHMSA, MARAD, and NHTSA) with weaknesses in data protection and privacy to update the status and develop POA&Ms to address the weaknesses.
7	Update specialized training guidance in DOT Cybersecurity Action Memos policy and DOT Cybersecurity Compendium policy to clearly define requirements.
8	Enhance security awareness training policy to define processes to tailor this training to DOT's unique environment and use feedback to enhance its program.

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

Appendix C: Organizations Visited or Contacted

Office of the Secretary (OST)

Office of the Chief Information Officer (OCIO)

Federal Aviation Administration (FAA)

Federal Highway Administration (FHWA)

Federal Motor Carrier Safety Administration (FMCSA)

Federal Railroad Administration (FRA)

Federal Transit Administration (FTA)

Maritime Administration (MARAD)

National Highway Traffic Safety Administration (NHTSA)

Office of Inspector General (OIG)

Pipeline and Hazardous Materials Safety Administration (PHMSA)

Appendix D: Representative Subset of Sampled Systems

FAA

	System Name	Impact Level	Contractor System
1	AIT Databases	High	No
2	Civil Aviation Registry Applications	High	No
3	Enhanced Flight Standards Automation System	High	No
4	Aeronautical Mobile Communications System	Moderate	Yes
5	Air Traffic Control Beacon Indicator 6	Moderate	No
6	Airport Cable Loop System	Moderate	No
7	Airport Surface Surveillance Capability	Moderate	No
8	Airport Surveillance Radar 8 with Common Terminal Digitizer	Moderate	No
9	Alaskan Satellite Telecommunications Infrastructure	Moderate	No
10	Common Automated Radar Terminal System	Moderate	No
11	Display System Replacement	Moderate	No
12	Dynamic Ocean Tracking System Plus	Moderate	No
13	ABA Documentum	Moderate	No
14	Accident Incident Data System	Moderate	No
15	Aeronautical Center Security Management System	Moderate	No
16	AFN Infrastructure at Equinix DC-3/FCS Colocation	Moderate	No
17	Air Traffic Safety Oversight Service Credentialing System	Moderate	No
18	Airman Testing Standards	Moderate	No
19	Airports Compliance Application Suite	Moderate	No
20	AML Logistics Center Local Area Network	Moderate	No
21	ASH External Web Portal	Moderate	No
22	ASH Web Portals (FSRS, PASS, WEB-DG, IMS, ASH SAVI) Applications	Moderate	No
23	Automated Vacancy Information Access Tool for Online Referral	Moderate	No
24	Aviation Safety Knowledge Management Environment Engineering Design and Production Approval	Moderate	No
25	Certification Project Notification	Moderate	No
26	Command and Control Communications Division LAN	Moderate	No
27	Cost Accounting System	Moderate	No
28	Enhanced Radar Intelligent Tool	Moderate	No
29	Enterprise Services Center Business Systems	Moderate	No
30	Enterprise Services Center Cloud Enclave	Moderate	No
31	Advanced Electronic Flight Strips	Low	No
32	Airport Management Tool	Low	No
33	Airports Geographic Information System	Low	No
34	Automated Contingency Tool 2	Low	No
35	Automated Weather Observation System Data Acquisition System	Low	No
36	Corporate Investment Management System	Low	No
37	FAA Administrative Voice Enterprise Services	Low	Yes
38	FAA Blackboard	Low	Yes
39	FAA Motor Vehicle System	Low	No

	System Name	Impact Level	Contractor System
40	Facility Power Panel System	Low	No
41	Instrument Flight Procedures Automation - Enterprise Services Center	Low	No

OST

	System Name	Impact Level	Contractor System
1	Common Operating Environment	High	Yes
2	Volpe Physical Access Control System	High	Yes
3	Airline Performance Economic Information System	Moderate	Yes
4	Facilities (Energy Management System)	Moderate	Yes
5	Facilities and Building Management System	Moderate	Yes
6	Personnel Security Enterprise System	Moderate	No
7	Image Management System	Low	Yes

PHMSA

	System Name	Impact Level	Contractor System
1	PHMSA Portal System	Moderate	Yes
2	Safety Monitoring and Reporting Tool	Moderate	Yes

FHWA

	System Name	Impact Level	Contractor System
1	Engineer's Estimate Bidding Award Construction System	Moderate	Yes
2	Fiscal Management Information System 5	Moderate	Yes

FMCSA

	System Name	Impact Level	Contractor System
1	Enforcement Management Information System	Moderate	Yes
2	Pre-Employment Screening Program	Moderate	Yes

FRA

	System Name	Impact Level	Contractor System
1	Railroad Safety Information System	Moderate	No
2	Web Information Services	Moderate	No

FTA

	System Name	Impact Level	Contractor System
1	Financial Management System	Moderate	Yes
2	Transit Integrated Appian Development Platform	Moderate	Yes

MARAD

	System Name	Impact Level	Contractor System
1	Comprehensive Academic Management System	Moderate	Yes
2	Maritime Service Compliance System	Moderate	Yes

NHTSA

	System Name	Impact Level	Contractor System
1	NHTSA020: Artemis	Moderate	Yes
2	NHTSA119 Grants Management Solution Suite[39]	Moderate	Yes

OIG

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

[39] GMSS replaced the Fatality Analysis Reporting Systems (FARS) during the audit, since FARS was retired and subsumed into another system during the audit period.

Appendix E: Management Comments

1200 New Jersey Avenue, SE
Washington, DC 20590

U.S. Department of Transportation

Office of the Secretary of Transportation

Subject: **ACTION**: Management Response to OIG Draft Report - Federal Information Security Modernization Act (FISMA) for Fiscal Year 2019

From: Andrew R. Orndorff
Associate Chief Information Officer /
Chief Information Security Officer
Office of the Chief Information Officer

ANDREW R ORNDORFF

Digitally signed by ANDREW R ORNDORFF
Date: 2019.09.16 13:15:10-04'00'

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

For Fiscal Year 2019, the Department of Transportation (Department or DOT) maintained an overall rating of "Managing Risk" from the Department of Homeland Security (DHS) under the framework and risk management assessment methodology established under Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." During this time, the Department also began a significant information technology (IT) transformation initiative to realign commodity IT and shared services for improved efficiencies, improved performance and service delivery, and reduced cybersecurity risks. Specific achievements include the following:

- protected approximately 15,000 users and their data via the implementation of a data loss prevention solution to assess and monitor DOT file servers for sensitive information, and alert operators to unsecured or unauthorized data for corrective action;
- significantly reduced website vulnerabilities through the implementation of a new web vulnerability scanning and management platform that assesses 346 agency websites and supports remediation of critical, high, and moderate vulnerabilities;
- improved security for more than 72 percent of the desktops, laptops, and tablets supported by the DOT Office of the Chief Information Officer (OCIO) resulting from upgrades to Microsoft Windows 10 from Windows 7, as of the end of July 2019; and

- mitigated a variety of threats and attacks through deployment of web application firewall protections for websites hosted on the DOT enterprise platform.

There continues to be a disconnect between the DHS and OIG assessments of the Department's cybersecurity posture and program. The Department has made progress on Federal cybersecurity metrics, internal measurement and reporting of cybersecurity performance and risks, automation of capabilities, and outcomes including no major cybersecurity incidents to date, and no outstanding critical and high weaknesses on Internet- facing endpoints.

Cybersecurity remains a top priority for the Department, with attention and support from senior agency leadership. The OCIO will continue efforts to cost-effectively reduce risks across the enterprise, leveraging modernization and realignment of commodity and enterprise functions and resources to achieve these gains. We look forward to sharing the results of our efforts with the OIG during FY 2020.

Upon review of the OIG draft report, we concur with recommendation 10, as written and will complete planned actions by January 10, 2020. We partially concur with recommendations 1 – 9 and 11 – 14. as discussed below:

- We partially concur with recommendation 1 and provide an alternative action to address the finding. The Department does not consider the use of its limited IT and cybersecurity resources to reprocess Plan of Action and Milestones (POAMs) already closed to be a cost-effective action to address improvement to DOT POAM management processes. The auditors did not acknowledge DOT's tailored implementation of the National Institute of Standards and Technology (NIST) requirements for the management of POAMs, as documented in the Weakness Management Guide, specifically section 2.3, which is designed to strike a balance between risk, impacts to program or mission operations, and the cost of implementation. While we do not agree to perform a review of all POAMs closed during the audit period, we plan to develop and implement a risk-based oversight approach to review and assess the quality of closed POAMs from the last cycle and update related policy, as appropriate. The Department plans to complete these actions by September 8, 2020.

- We partially concur with recommendation 2 and offer an alternative action to address this finding. It is not necessary to include e-mail and calendar items in the Cybersecurity Assessment and Management (CSAM) system as evidence in support of recommendations to close, as other documents can provide sufficient evidence, such as meeting minutes. Including e-mail and calendar items in CSAM would duplicate records maintained within the Department's e-mail system(s), as the official repository of those records, and these records may not be authoritative evidence of meetings or other actions taken. The unnecessary duplication of records in multiple systems creates unnecessary and, therefore, unacceptable, risk to the Department's information assets.

  As such, our proposed alternative action is to enhance implementation guidance regarding evidence for POAM closure to include meeting minutes, and/or other

appropriate documentation, without the inclusion of e-mail or calendar records. We plan to complete these actions by April 6, 2020.

- We partially concur with recommendation 3 with the observation that the DOT Cybersecurity program and the DOT Privacy program function as separate and equal, but parallel risk management programs, with corresponding controls and documentation assessed in accordance with their respective policies and subject matter expertise.

  As an alternative action, the Department will work with applicable Component representatives to review assessment and authorization processes and implement a process to ensure updated security plans, authorities to operate (ATOs), and risk assessments are reviewed and updated to reflect applicable system controls, and technical vulnerabilities, and that current risks are clearly presented to the authorizing officials. We will require the Federal Aviation Administration (FAA) to ensure the same for its systems. We plan to complete these actions by December 2, 2020.

- We partially concur with recommendation 4 as the recommendation is not implementable as written. We propose an alternate action that the Department will ensure all applicable Component system security plans and assessments reflect the system architecture, and applicable security controls are properly evaluated. We will require the FAA to ensure the same for its systems. We plan to complete these actions by July 6, 2020.

- We partially concur with recommendation 5 as the auditors did not provide sufficient evidence of testing of these controls and findings to the Department. Per DOT Order 1351.40, "COE Services Management Policy", which lays out the scope and responsibilities for IT Shared Services provided via the COE:

  - Page 2: The DOT OCIO IT Shared Services (ITSS) organization provides IT infrastructure services, including but not limited to network services, to customers of the COE.
  - Page 11: Section 40.5 clearly lays out the respective roles and responsibilities of the Associate CIO for ITSS, ITSS staff, and the Components with respect to use, management, and security of IT Shared Services, including IT infrastructure.

  Consistent with that policy and per the requirements of DHS Binding Operational Directive (BOD) 19-02, the Department maintains an inventory of IP address networks and allocations, which must be submitted to DHS when changes are made to ensure that DHS is able to assess for traffic leakage as part of the National Cybersecurity Protection System (NCPS) / EINSTEIN program, and to support DHS scanning of DOT Internet-facing endpoints for vulnerabilities as required by the BOD.

  Furthermore, the Department, as reported in prior audits, has been modernizing the architecture and management of DOT OCIO-managed networks via the

Network Assessment Risk Mitigation (NARM) initiative. The systems developed under NARM maintain near-real-time inventories of network infrastructure, including physical locations and other attributes, and can detect when new, unrecognized or unauthorized network infrastructure is introduced into the environment. The new architecture provides for improved segmentation, and the opportunity to implement future network requirements consistent with Federal and DOT policy.

Lastly, the Department, consistent with the requirements of the Federal Continuous Diagnostics and Mitigation (CDM) program, has begun tagging endpoints on DOT networks to attribute them to specific DOT Components and systems in the Department's system inventory. This is in support of the Department's assessment and management of risks, reporting to the DOT and DHS enterprise cybersecurity dashboards, and in support of future security automation to improve DOT security authorization and continuous monitoring processes.

Because the intent of the recommendation is addressed by existing policy, we request closure within 30 days of the final report's issuance.

- We partially concur with recommendation 6 on the basis that:

    - The auditors did not review the Department's Common Operating Environment (COE) Services Management Policy (DOT Order 1351.40) that states that IT infrastructure is a shared service, including networks (Section 40.2);
    - The auditors did not provide sufficient evidence of inadequate network segmentation in discussion papers, draft notices of findings and recommendations, or other working papers to the Department;
    - The auditors did not review the Department's network modernization initiative and scope – the Network Assessment Risk Mitigation (NARM) initiative – which specifically includes software-defined networking and network segmentation as design requirements; and,
    - The auditors did not review the Department's implementation of modernized systems in the authorized Microsoft Azure and Amazon Web Servers (AWS) cloud environments, which by design implement network segmentation as part of the operating environment configured for each system and application.

  Because the intent of the recommendation is addressed by existing policies and practices, we request closure of this recommendation within 30 days of the final report's issuance.

- We partially concur with recommendation 7 with the observation that this recommendation is a duplication of recommendation 15 from the FISMA 2014 audit regarding identity and access management, of which Personal Identify Verification (PIV) authentication is a part, and for which the Department has already issued policy, developed or acquired capabilities, and is in the process of implementing. The Department does not believe that the recommendation as written will achieve the desired result because the recommendation does not

address the potential root causes attributed to the current state of progress – including lack of funding, competing priorities, or shortage of personnel. As a result, the Department proposes an alternative action to update its existing criteria to both better document how DOT information systems already reap the benefits of the existing enterprise identity and access management solutions—to include Active Directory and Azure Active Directory, MyAccess, the Office of Management and Budget's (OMB) Max Authentication Service, and the General Services Administration's (GSA) login.gov service—through control inheritance, to provide additional clarity as to specific solutions or services each applicable Component may leverage and the use cases under which they may be applied, to provide clarity on the exception and risk acceptance process for mission systems that cannot leverage the enterprise infrastructure, and to require prioritization of funding and other resources within future investment updates and budget requests. We will complete these actions by April 6, 2020.

- We partially concur with recommendation 8, as the Departmental Chief Privacy Officer (CPO) has established a clear process and guidance for the completion of privacy risk management activities. As an alternative action to address the finding, the Department plans to assess the capacity and capability of the Departmental and component level Privacy programs to implement required functions and processes and develop a corrective action plan based on the results of the assessment. We will complete these actions by August 3, 2020.

- We partially concur with recommendation 9 and propose an alternative action noting that the auditors did not report a weakness to the Department regarding timely notification and reporting of cybersecurity incidents. As a result, the Department will update its processes to ensure the timely update and resolution of cybersecurity incidents. We plan to complete actions by February 3, 2020.

- We partially concur with recommendation 11, noting that the Department provided evidence that applicable DOT Components are not required to develop Component-level policy, and may inherit from Departmental policies and procedures, as is consistent with cost-effective implementation of the NIST Risk Management Framework, including:

    - DOT Order 1351.37, Departmental Cybersecurity Policy
        - Section 37.5.11.1: DOT Component Administrators must ensure "…a Component Cybersecurity Program is developed within their organizations in accordance with the Departmental Cybersecurity Policy".

        - Section 37.5.14.15: Component Information System Security Managers (ISSMs) are responsible for "…Implementing Departmental information security policies, procedures, and control techniques to address all applicable requirements";

    As a result, we propose an alternative action to issue updated policy to clarify Component responsibilities for IT policies, including cybersecurity, and

companion implementation guidance. We plan to complete actions by April 6, 2020.

- We partially concur with recommendation 12 and propose an alternative action, consistent with DOT policy, to require that the FAA review its cybersecurity incident response plan on an annual basis and the Department will ensure that applicable Components are properly accounted for in a revised DOT enterprise-wide incident response plan. We plan to complete the planned actions by July 6, 2020.

- We partially concur with recommendation 13 and propose an alternate action noting that the condition the auditors identified with the DOT Continuity of Operations Plan (COOP) plan was not a finding, as the provided plan was only approved by the Department, and submitted to the Federal Emergency Management Agency (FEMA), in August 2018—less than 12 months from the date of the auditors' review. The Department will ensure that the DOT COOP plan incorporates additional context and information regarding Departmental Information System Contingency Plans. We plan to complete these actions by October 2, 2020.

- We partially concur with recommendation 14 and provide an alternative action noting that the auditors did not acknowledge the enterprise recovery time and recovery point objectives defined in the DOT COOP plan, which OCIO considers to be an inheritable control and parameter for contingency planning. The Department will ensure that the DOT COOP plan provides additional context on the linkage between organizational business impact assessments (BIAs) and system-level BIAs, and that documentation is updated appropriately. We plan to complete these actions by October 2, 2020.

We appreciate the opportunity to comment on OIG's draft report. If you have any questions, please contact Andrew R. Orndorff, Chief Information Security Officer (CISO), at 202-366- 7111.

U.S. DOT OIG Fraud & Safety Hotline

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

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

Our Mission

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

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

www.oig.dot.gov