U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

DOT Has Not Met Federal Targets for Implementing Components of Its Information Security Continuous Monitoring Program

Report No. FI2019014

December 4, 2018

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

DOT Has Not Met Federal Targets for Implementing Components of Its Information Security Continuous Monitoring Program

Self-initiated

Department of Transportation | FI2019014 | December 4, 2018

What We Looked At

The Office of Management and Budget (OMB) requires Federal agencies to implement Information Security Continuous Monitoring (ISCM), which entails the near real-time detection of cybersecurity risks, threats, and malicious activity. ISCM enables agencies to more effectively address evolving, frequent, and increasingly aggressive cybersecurity attempts to compromise Federal information systems. A large number of systems at the Department of Transportation (DOT) contain sensitive data that require protection; accordingly, we initiated this audit. Our audit objectives were to assess (1) how DOT's ISCM program conforms to OMB and National Institute of Standards and Technology requirements and (2) the status and progress of DOT's implementation of its ISCM program. This review also supports our annual audit mandated by the Federal Information Security Modernization Act.

What We Found

DOT's program lacks a procedure for verifying Federal Aviation Administration (FAA) performance data reported to OMB. While DOT has met the requirement to submit quarterly reports, we identified significant errors in one submission. The Department also lacks adequate procedures for providing accurate submissions to OMB. In addition, FAA has not yet completed phase 1 of the Continuous Diagnostics and Mitigation Program, which targets the management of cybersecurity assets and activities. Finally, FAA does not have procedures for reporting on or validating its Cross Agency Priority goal data and cannot be certain those data are accurate.

Our Recommendations

DOT concurred with our three recommendations to improve its ISCM program.

All OIG audit reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Legal, Legislative, and External Affairs at (202) 366-8751.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: December 4, 2018

Subject: ACTION: DOT Has Not Met Federal Targets for Implementing Components of Its Information Security Continuous Monitoring Program | Report No. FI2019014

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

To: Federal Aviation Administrator
DOT Chief Information Officer

The Office of Management and Budget (OMB) requires Federal agencies to implement Information Security Continuous Monitoring (ISCM), which entails the near real-time detection of cybersecurity risks, threats, and malicious activity. ISCM enables agencies to more effectively address evolving, frequent, and increasingly aggressive cybersecurity attempts to compromise Federal information systems.

As a large number of systems at the Department of Transportation (DOT) contain sensitive data that require protection, we initiated this audit. Our audit objectives were to assess (1) how DOT's ISCM program conforms to OMB and National Institute of Standards and Technology (NIST) requirements and (2) the status and progress of DOT's implementation of its ISCM program. For our first objective, we focused on OMB's requirements for performance-based goal metrics since we cover ISCM in our annual audits mandated by the 2014 Federal Information Security Modernization Act (FISMA).[1] For our second objective, we limited our focus to the ISCM program at the Federal Aviation Administration (FAA), which owns over 300 (about 70 percent) of DOT's major information systems. This audit also supports our fiscal year (FY) 2017 FISMA audit.

[1] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) amends the 2002 Federal Information Security Management Act to, among other things, (1) reestablish the oversight authority of the OMB Director for agency information security policies and practices and (2) set authority for the Secretary of the Department of Homeland Security to administer the implementation of policies and practices for information systems.

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the entities we visited or contacted.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me or Abdil Salah, Program Director, at (202) 366-8543.

cc: The Secretary
Deputy Assistant Administrator for Information Services/
Chief Information Officer, FAA
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

Results in Brief

DOT's ISCM program lacks a procedure for verifying FAA's performance data reported to OMB.

As part of its ISCM program, and in compliance with OMB requirements, DOT submits quarterly reports on its Cross Agency Priority (CAP)[2] performance-based goal metrics to OMB and the Department of Homeland Security (DHS). While DOT has met the requirement to submit quarterly reports, we identified significant errors in one submission. In addition, the Department lacks adequate procedures for providing accurate submissions to OMB. The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*[3] requires agencies to use quality information[4] to communicate internally or externally and to make informed decisions, and agency management to evaluate sources of data for reliability. However, the Department's submission for the fourth quarter of FY 2016 did not accurately report the data FAA provided. FAA reported to DOT that 23 percent of its assets could not block unauthorized software from executing, but DOT reported to DHS that 100 percent of the Department's assets had this capability. DOT also reported that 86 percent of its assets had been assessed for vulnerabilities using Security Content Automation Protocol (SCAP)-validated products. However, 75 percent of those assets are at FAA, which reported to the Department that less than 20 percent of its assets had been checked with a SCAP-validated product. DOT's Chief Information Security Officer (CISO) stated that these discrepancies were caused by errors his office made in its report to DHS. We noted that DOT did not have procedures to verify the quality of this information or access to the tool used by FAA. Due to errors in calculating and reporting key performance-based metrics, OMB and Department leadership might use inaccurate data to make risk-based decisions.

Weaknesses in FAA's ISCM implementation may impact the quality of its performance reports.

Federal guidelines required Government agencies to fully implement phase 1 of the DHS-administered Continuous Diagnostics and Mitigation (CDM) Program by the third quarter of FY 2014. FAA did not meet this milestone. FAA officials attributed the delays to another agency, which has a formal agreement with FAA

[2] OMB defines Cross-Agency Priority (CAP) goals as a tool used by leadership to accelerate progress on a limited number of Presidential priority areas where implementation requires active collaboration among multiple agencies.

[3] Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G), September 2014.

[4] Federal internal control standards state that quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis.

to install the CDM program. In May 2017, they told us they might not meet the new target date for full operational compliance, November 30, 2018, “as additional information is gathered through the deployment process.” According to OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems,” agencies should evaluate capability gaps, upgrade their infrastructure, deploy new products to support ISCM, and automate their submissions of security-related information to OMB and DHS. However, FAA lacks procedures for reporting on CAP performance-based goal metrics that define the requirements for determining the operating systems to be monitored; the tools monitoring each information system; and the steps for verifying the accuracy and completeness of the CAP goal metrics. The Agency also lacks controls for verifying, validating, and retaining the data used to report on CAP performance-based goal metrics. FAA officials said they do not validate the data that are output from monitoring tools because CDM phase 1 is not fully operational. As a result, FAA may not have the valid, accurate and complete information it needs to make risk-based decisions in a timely and effective manner.

We are making recommendations to help DOT and FAA report valid, accurate, and complete metrics about their ISCM programs to OMB and DHS.

Background

In our FY 2017 FISMA audit, we reviewed the *Detect* controls DOT uses to identify cybersecurity incidents as part of ISCM. We reported that DOT, for the most part, has formalized and documented its policies, procedures, and strategies for ISCM; however, they are not consistently implemented throughout the Department. Based on this, we determined that DOT was at the *Defined* maturity level—the second lowest tier of the maturity model for information security—for its *Detect* controls. This represented an improvement over the results of our FY 2016 FISMA audit, where we found DOT’s *Detect* controls were at the lowest level of maturity.

According to NIST Special Publication (SP) 800-137, “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,” the Chief Information Officer (CIO) leads the organization’s ISCM program and ensures that it is implemented effectively. The CIO establishes expectations and requirements; works closely with authorizing officials to provide funding, personnel, and other resources; and maintains high-level communications and working-group relationships with organizational entities. In addition, DOT’s Security Authorization and Continuous Monitoring Performance Guide specifies the following responsibilities for the Department’s CISO and the Components’ (Operating Administrations’) information systems security managers:

- Develop an ISCM strategy;
- Develop an ISCM policy, procedure, and standards;
- Implement and maintain ISCM capabilities;
- Monitor weaknesses and remediation progress.

OMB M-14-03 requires agencies to evaluate capability gaps, upgrade their infrastructure, and deploy new products, as needed, to support ISCM and automate the submission of security-related information to OMB and DHS. As outlined in the U.S. Government Concept of Operations (CONOPS) for ISCM, an agency has a variety of options when implementing its ISCM technical architecture, including leveraging the services and products offered by the CDM program; using the agency's existing products and services; or implementing a hybrid approach.

The CDM program enhances Government network security through an automated process that tests controls and tracks progress. CDM has four phases;[5] phase 1 focuses on managing "what is on the network," i.e., hardware assets, software assets (including malware management), configuration settings, and common vulnerabilities. ISCM also requires agencies to install a CDM dashboard that displays cybersecurity information relative to their security posture—based on data collected from the monitored information systems, devices, and other assets.

In addition, OMB requested that agencies provide CAP performance-based goal metrics for their ISCM activities in the fourth quarter of FY 2016. OMB's FY 2017 CIO FISMA metrics[6] align with the Administration's high-priority CAP goal metrics for information security. The 24 Federal agencies covered by the Chief Financial Officers (CFO) Act must report on the status of these CAP goal metrics on a quarterly basis, at a minimum, and OMB publishes progress updates in its quarterly Cybersecurity CAP Goal Report on Performance.gov. Agencies are expected to explain any metric that does not meet OMB's established CAP goal targets of 95 percent or above. Table 1 identifies the CAP goal metrics for FY 2016.

[5] The CDM phases are as follows: phase 1, what is on the network; phase 2, who is on the network; phase 3, what is happening on the network; and phase 4, how data are protected.

[6] CIO FISMA metrics focus on assessing departments' or agencies' progress in achieving outcomes that strengthen Federal cybersecurity.

Table 1. OMB’s CAP Goal Metrics for FY 2016

Summary of FISMA CAP Goal Targets and Methodology				
Capability	**Target %**	**FY 2016 Annual FISMA CIO Metrics**	**FY 2015 Annual FISMA CIO Metrics**	**Agency Calculation**
Information Security Continuous Monitoring (ISCM)				
Hardware Asset Management	≥ 95%	1.4, 3.16	2.2, 2.3	Both results must be greater than or equal to target.
Software Asset Management	≥ 95%	1.5, 3.17	2.6, 2.7	Both results must be greater than or equal to target.
Vulnerability and Weakness Management	≥ 95%	2.2	2.11	Result must be greater than or equal to target.
Secure Configuration Management	≥ 95%	2.3.4	2.10.6	Result must be greater than or equal to target.
Identity and Credential Access Management (ICAM)				
Unprivileged Network Users	≥ 85%	2.4.1	3.1.1	Result must be greater than or equal to target.
Privileged Network Users	100%	2.5.1	3.2.1	Result must be greater than or equal to target.
Anti-Phishing and Malware Defense				
Anti-Phishing Defense	≥ 90%	2.19.1, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6	4.2, 4.5, 4.6, 4.7, 4.9, 4.13, 8.2.1	Top 5 results must be greater than or equal to target.
Malware Defense	≥ 90%	3.8, 3.8, 3.9, 3.10, 3.11.1	4.3, 4.4, 4.8, 4.11, 6.1.4	Top 3 results must be greater than or equal to target.
Other Defenses	≥ 90%	3.12, 3.13, 3.14, 3.15	4.1, 4.10, 4.12, 4.14	Top 2 results must be greater than or equal to target.

Source: OMB and DHS

NIST SP 800-137 directs Government agencies to develop procedures for analyzing and reporting the results of their assessments and monitoring activities. This includes the specific staff who should receive ISCM reports; the content, format, and frequency of the reports; and any tools to be used, as well as requirements for analyzing and reporting results of controls, whether or not they are automated. SP 800-137 also directs agencies to collect additional data to supplement or clarify security-related information, and knowledgeable staff to select, implement, operate, and maintain the tools and technologies that monitor security status, as well as all underlying security controls; interpret the monitoring data; and determine appropriate remediation.

DOT's ISCM Program Does Not Have a Procedure To Verify That FAA's Performance-Goal Metric Data Comply With OMB Requirements

DOT's FY 2016 report on its CAP performance-based goal metrics did not accurately reflect the status at the Department's largest agency, FAA. In accordance with DOT's standard operating procedures for addressing FISMA requirements, each quarter the Office of the Chief Information Officer (OCIO) emails a data-request spreadsheet to the Operating Administrations. The request includes a series of questions referencing the CAP performance-based goal metrics they are to provide. DOT used the spreadsheet to prepare and submit its FY 2016 CAP goal metrics to DHS and OMB, as required by OMB.

GAO's *Standards for Internal Control in the Federal Government* requires agencies to use quality information to communicate internally or externally and to make informed decisions, and agency management to evaluate sources of data for reliability. According to the standards, quality information is appropriate, complete, and accurate, among other things.

The Department's procedures direct the OCIO to compare the results received from the Operating Administrations with the ISCM tools in place for DOT. However, they do not include steps for verifying the accuracy and completeness of FAA's CAP goal metrics submission because FAA uses a tool that the OCIO is not authorized to access. As a result, the Department's submission to OMB and DHS might not have accurately represented the agency's aggregate performance for the respective metrics. For example,

- For the fourth quarter of FY 2016, DOT's response to question 3.17[7] indicated that all (100 percent) of its Government-furnished equipment (GFE) and mobile assets[8] were covered by a software asset management

[7] FY 2016 CIO FISMA metric question 3.17: Number of Government-furnished equipment (GFE) endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by a software asset management capability to detect, alert, and/or block unauthorized software from executing (e.g., certificate, path, hash value, services, and behavior-based whitelisting solutions).

[8] FY 2016 CIO FISMA metric question 1.2.1: Number of GFE endpoints connected to the organization's unclassified network(s). Question 1.2.2: Number of GFE mobile assets connected to the organization's unclassified network(s).

capability to detect, alert, and/or block unauthorized software from executing. However, FAA's response stated that 15,052 of 65,346 (23 percent) assets did not have capability to detect, alert, and/or block unauthorized software from executing.

- For the fourth quarter of FY 2016, FAA's response to question 2.2[9] stated that less than 20 percent of its assets were assessed for vulnerabilities using SCAP-validated products. FAA represents approximately 75 percent (85,102 of 113,315) of DOT assets. However, in its answer to question 2.2, DOT reported that 86 percent of its assets were assessed for vulnerabilities using SCAP-validated products.

DOT's CISO stated that these discrepancies were caused by errors his office made in its report to DHS. We also found that DOT does not have procedures to detect such errors. As it also lacks verification and validation steps for reporting FAA's metrics, the Department cannot ensure that it will submit accurate and complete CAP-related reports about its hardware and software assets, configuration settings, and cybersecurity vulnerabilities. Furthermore, DOT's leadership team might not have accurate and up-to-date information about the strengths and weaknesses in the Department's cybersecurity posture. Finally, due to errors in calculating and reporting required performance-based metrics OMB, Department leadership, and other stakeholders might use inaccurate data to make risk-based decisions.

Weaknesses in FAA's ISCM Implementation May Impact the Quality of Its Performance Reports

FAA has not yet completed CDM phase 1, which targets the management of cybersecurity assets and activities. In addition, FAA does not have procedures for reporting on or validating its CAP goal data and cannot be certain those data are accurate.

FAA's Implementation of CDM Phase 1 Is Delayed

FAA has yet to establish full operational capabilities for CDM phase 1. While the Agency has implemented tools on most portions of its network, it has missed

[9] FY 2016 CIO FISMA metric question 2.2: Percent (%) of the organization's unclassified network(s) assessed for vulnerabilities using Security Content Automation Protocol (SCAP)-validated products.

target action dates for the CDM dashboard installation, Splunk, IBM BigFix, ForeScout CounterAct for Mission Support, and R&D Domain. The CDM program gives agencies the capabilities and tools to identify and prioritize cybersecurity risks; phase 1 targets the management of hardware assets, software assets, configuration settings, and common vulnerabilities. In May 2017, FAA told us, "The Phase 1 products are being deployed into the Mission Support and Research & Development (R&D) domains. Deployment is scheduled for completion in FY 2018 (currently 30 November); however, this milestone (Full Operational Capability) may be delayed as additional information is gathered through the deployment process."

FAA officials also reported that the Agency and DOT had a Memorandum of Agreement with another agency to install the CDM dashboard by May 31, 2017. However, technical issues are impeding the installation, and FAA informed us that until the root causes of those issues are identified and resolved, the Agency cannot schedule a new implementation date for the dashboard. Due to this delay, FAA may not be able to make effective and timely risk-based decisions.

FAA Lacks Procedures for Reporting on CAP Performance-Based Goal Metrics

FAA does not have procedures to guide staff who prepare reports on the Agency's cybersecurity CAP goal metrics. Such procedures, outlined in NIST SP 800-137, would help the Agency review the accuracy and completeness of the data it collects for ISCM. FAA's LOBs use specific tools—McAfee Vulnerability Manager, AirWatch, Belarc, and NAC Forescout—to collect and report on CAP goal metrics for their hardware assets, software assets, vulnerabilities, and configuration settings. According to FAA officials, the Agency also uses this information to determine risk. However, FAA lacks reporting procedures to help ensure the data are accurate and complete.

FAA also does not have criteria to help personnel determine which tools to use when monitoring information systems or collecting data for the CAP goal metrics. In one example, an FAA official could not explain why one tool was used to track only the Windows 7.x operating system. In another example, the Belarc system owner did not know that tool was being used to collect information for metrics

1.4,[10] 1.5,[11] 2.3.4,[12] and 3.17 (see table 1). The system owner said that Belarc had been procured primarily to monitor software licenses.

Furthermore, when we tested a random sample of 9 of 20 tools at 2 of the 6 FAA LOBs with the most network access points and systems, we found that 100 percent of the sample lacked formal and documented procedures to assess accuracy and completeness of CAP goal metrics data. NIST requires organizations to develop procedures for analyzing and reporting assessment and monitoring results. FAA officials told us the Agency's Mission Support and R&D divisions participate in the DHS CDM program; however, CDM phase 1 is not fully deployed. As such, FAA relies on two different tools, McAfee Vulnerability Manager and Belarc, to collect and report on its CAP goal metrics for ISCM.

FAA's lack of procedures to guide its analysis of and reporting on CAP performance-based metrics could result in DOT having incorrect information about the management of its hardware assets, software assets, configuration settings, and cybersecurity vulnerabilities. In addition, FAA's and DOT's leadership teams might not have accurate and up-to-date information about the level of performance and existing gaps in the cybersecurity posture.

FAA's CAP Performance-Based Goal Metrics Data Are Unreliable

FAA cannot rely on the data it uses to report on its CAP goal metrics and make risk-based decisions. During our review of FAA's processes for checking the accuracy and completeness of its reports, we found:

- FAA did not collect metrics from some of its five LOBs. Agency officials told us this was due to insufficient oversight from FAA management. For example, in the fourth quarter of FY 2016, FAA did not collect this information from three LOBs (ASH AEO, ASH AIN, and ANG).[13] And in the first quarter of FY 2017, FAA did not request CAP goal metrics from ANG or metric 2.2 from ESC.[14]

[10] FY 2016 CIO FISMA metric 1.4: Number of GFE hardware assets (from 1.2.) covered by an automatic (e.g., scans/device discovery processes) hardware asset inventory capability at the enterprise level.

[11] FY 2016 CIO FISMA metric 1.5: Number of GFE endpoints and mobile assets (from 1.2.1. and 1.2.2.) covered by an automated software asset inventory capability at the enterprise level.

[12] FY 2016 CIO FISMA metric 2.3.4: Number of assets in 2.3.1 covered by auditing for compliance with 2.3.2.

[13] ASH is the Office of Security and Hazardous Materials Safety. AEO is now Office of National Security Programs and Incident Response (AXE). ASH AIN is now Office of Investigations (AXI). ANG is the Office of NextGen (Next Generation Air Transportation System).

[14] ESC is the Enterprise Services Center.

- FAA submitted identical data for all the CAP performance-based goal metrics for the third and fourth quarters of FY 2016. Agency officials told us, "Based upon the DOT OCIO data call for 3rd and 4th quarter, DOT OCIO allows for reuse of FY16 Quarter 1 submissions unless the data has changed, and because there were no changes to the tools used to report the data, the FAA did not report updated numbers for the 3rd quarter to the 4th quarter." However, FAA did not provide evidence to show that the data for the third and fourth quarters remained the same.

- FAA does not have a process for validating data output from the following tools: McAfee Vulnerability Manager, AirWatch Mobile Device Management, Belarc, and NAC Forescout. For example, for metric 1.4, FAA did not validate the output from Belarc—which monitors hardware assets—by comparing it to the Automated Inventory Tracking System, which records and tracks the Agency's accountable property.

- FAA officials said they do not validate the output from monitoring tools because CDM phase 1 is not fully operational. Instead, the Agency uses existing tools intended for operational purposes—for example, Belarc is used for software licensing management—to collect data for the ISCM CAP goal metrics.

According to NIST, the value of automated tools and technologies, including those that perform gather, aggregate, and analyze data, depends on the operational processes that support their use.

FAA's use of unreliable data to report on its CAP performance-based goal metrics weakens the effectiveness of its ISCM program. This is particularly important as FAA uses the CAP results to make risk-based decisions about the protection of its networks and assets.

Conclusion

The Department of Transportation (DOT) faces sophisticated cyberattacks that can make its information systems and operations vulnerable. To combat these threats, DOT and the Federal Aviation Administration (FAA)—which houses most of the Department's IT assets—must monitor their systems using the methods and tools that are most likely to mitigate risk. The growing interaction between IT and operations makes it even more critical to collect comprehensive data about the Department's cybersecurity posture. According to the National Institute for Standards and Technology, a well-designed and well-managed ISCM program can transform a static and occasional assessment into a dynamic process that provides essential, near real-time information about cybersecurity. Senior leaders can use this information to make cost-effective, risk-based decisions regarding the operation of their information systems. DOT's and FAA's transition to a well-managed ISCM program is hindered by a lack of controls for analyzing data about their information systems as well as a less-than-rigorous data review process. Until DOT and FAA address these data issues, they will be unable to assess any progress in their efforts to deploy a consistently implemented ISCM program or have reliable data for risk-based decisions.

Recommendations

To improve the DOT's Information Security Continuous Monitoring Program, we recommend that the DOT Chief Information Officer

1. Update the Department's Federal Information Security Modernization Act standard operating procedures to include steps for verifying the accuracy and completeness of the Federal Aviation Administration's (FAA) Cross Agency Priority (CAP) goal metrics.

To improve the accuracy and completeness of the data FAA uses to report on its CAP goal metrics, we recommend that the Federal Aviation Administrator

2. Implement procedures that:

    a. Define the requirements for selecting the operating systems to be monitored;

    b. Define criteria for determining which tools should be used to collect data for the CAP goal metrics;

    c. Verify the accuracy and completeness of the CAP goal metrics.

3. Develop and implement controls for verifying, validating, and retaining data used to report on CAP performance-based goal metrics.

Agency Comments and OIG Response

We provided DOT with our draft report on October 11, 2018, and received its formal response on November 7, 2018, which is included as an appendix to this report. DOT concurred with our three recommendations and provided appropriate actions and completion dates. Accordingly, we consider all recommendations resolved but open pending completion of the planned actions.

Actions Required

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

Exhibit A. Scope and Methodology

We conducted this performance audit between February 2017 and October 2018 in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit covered DOT's implementation of its ISCM program and the reporting of CAP goal metric data to OMB. This audit also supported and augmented our FY 2017 FISMA audit. Audit criteria included DOT information technology policies and procedural guidance, FAA information technology procedural guidance, NIST, OMB requirements and guidance, and the CIO ISCM CONOPs version 1.0. Stakeholders included the Department's CIO and CISO, as well as FAA information system security managers and system and program owners. Our audit objectives were to assess (1) how DOT's ISCM program conforms to OMB and NIST requirements and (2) the status and progress of DOT's implementation of its ISCM program. We added a focus on the program at FAA because our annual reports[15] on DOT's compliance with FISMA have found that some of the Department's most significant cybersecurity challenges are at FAA.

To conduct our work, we reviewed DOT's and FAA's ISCM policies in conjunction with guidance from OMB, NIST, and the CONOPS. We visited DOT offices in Washington, DC; the Cyber Security Management Center in Leesburg, VA; as well as FAA field offices in Atlanta, GA, and Fort Worth, TX, to review FAA's process for reporting on CAP performance-based goal metrics. These locations were selected because they had the most network access points and systems. We collected FAA and DOT CAP goal metric submissions from FY 2016 through FY 2017 and interviewed personnel in the offices of the CIO and CISO, as well as information security managers, system owners, and program owners.

We obtained a listing of tools and systems for FAA's six LOBs from the Agency's Audit Liaison. We stratified the listing of tools according to LOB and selected a probability proportional to size with a replacement sample of tools from each stratum, where size was the number of systems for which a particular tool was used within an LOB. We selected a total of 36 of 74 tools that had 175,937 of 287,771 systems in the universe. We only tested 9 out of 20 tools—used on 149,441 systems (64 percent) of 234,510 systems—at 2 LOBs, because those LOBs had the most network access points and systems. The number of systems

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

reported to us might not be reliable because Agency officials could not show us how they arrived at that number.

To determine the status and progress of DOT's implementation of the ISCM program, we reviewed previous recommendations in our FISMA-focused reports and identified the status of the ISCM-related recommendations. We also obtained FAA project plans and assessed the implementation of the milestones and due dates.

Exhibit B. Organizations Visited or Contacted

Department of Transportation

Cyber Security Management Center, Leesburg, VA

Office of the Chief Information Officer, DOT Headquarters, Washington, DC

Federal Aviation Administration

FAA Headquarters, Washington, DC

FAA Field Office, Atlanta, GA

FAA Field Office, Fort Worth, TX

Exhibit C. List of Acronyms

CAP	Cross Agency Priority
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CONOPS	U. S. Government Concept of Operations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FISMA	Federal Information Security Modernization Act
FY	fiscal year
GAO	Government Accountability Office
GFE	Government-furnished equipment
ISCM	Information Security Continuous Monitoring
LOB	Lines of Business
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
R&D	Research & Development
SCAP	Security Content Automation Protocol
SP	Special Publication (NIST)

Exhibit D. Major Contributors to This Report

ABDIL SALAH	PROGRAM DIRECTOR
SEVERIN PEFOUBOU	PROJECT MANAGER
SHAVON MOORE	INFORMATION TECHONOLOGY SPECIALIST
NILESHKUMAR PATEL	INFORMATION TECHONOLOGY SPECIALIST
JAMES MULLEN	INFORMATION TECHONOLOGY SPECIALIST
FRITZ SWARTZBAUGH	ASSOCIATE COUNSEL
JANE LUSAKA	WRITER-EDITOR
PETRA SWARTZLANDER	SENIOR STATISTICIAN
MAKESI ORMOND	STATISTICIAN

Appendix. Agency Comments

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

Memorandum

Subject: **INFORMATION:** Management Response to the Office of Inspector General (OIG) Draft Report on DOT's Information Security Continuous Monitoring (ISCM) Program

From: Andrew R. Orndorff
Associate CIO/Chief Information Security Officer

ANDREW R ORNDORFF

Digitally signed by ANDREW R ORNDORFF
Date: 2018.11.07 10:47:37 -05'00'

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

Protecting agency information systems and providing reliable data for decision-makers and in reporting are priorities for the U.S. Department of Transportation (DOT). We are committed to continued investment in people, processes and technology to mature DOT's ISCM program and capabilities, and to leveraging multiple sources of feedback to support continuous process improvement. DOT also acknowledges that it is impossible to have perfect data to support every risk-based decision, and that part of the risk conversation with DOT leadership, the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS) is understanding and communicating uncertainties and gaps in the data that is available so that the best decisions practicable may be made.

To that end, the Department undertook efforts during the FY2018 FISMA reporting cycle to improve data collection and validation processes, relying upon existing authorities and access codified within agency delegations. These actions included:

- leveraging capabilities specifically deployed for Continuous Diagnostics and Mitigation (CDM) to provide the baseline data for most of the reporting across the Department;
- instituting process changes to collect data from additional, appropriate sources to both validate, and augment, the baseline data being collected and reported;
- instituting changes within the Federal Aviation Administration (FAA) to establish processes for the retention of historical data consistent with FAA records management requirements; and
- initiating the deployment of specific CDM capabilities within the National Airspace System (NAS) domain.

Based on our review of the draft report, we concur with all three recommendations as written. We have already completed actions to implement recommendations 2 and 3 and will provide supporting documentation to the OIG requesting closure within 30-days after OIG issues the final report. We plan to complete actions to address recommendation 1 by September 30, 2019.

We appreciate the opportunity to review the OIG draft report. Please contact Andrew R. Orndorff, Associate CIO/Chief Information Security Officer, at 202-366-7111 with any questions.

U.S. DOT OIG

Fraud & Safety

☎ Hotline

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

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

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

www.oig.dot.gov