United States Government Accountability Office

Report to Congressional Committees

May 2023

CYBERSECURITY

DOT Defined Roles and Responsibilities, but Additional Oversight Needed

Accessible Version

GAO-23-106031

GAO Highlights

Highlights of GAO-23-106031, a report to congressional committees

May 2023

CYBERSECURITY

DOT Defined Roles and Responsibilities, but Additional Oversight Needed

Why GAO Did This Study

DOT was established in part to build, maintain, and oversee a vast national transportation system. To support its mission, the department relies on information systems to secure sensitive information.

The Infrastructure Investment and Jobs Act includes a provision for GAO to report on the cybersecurity roles and responsibilities of senior IT officials at DOT and its component operating administrations.

This report examines the extent to which DOT (1) has defined cybersecurity roles and responsibilities for department and component agency senior officials and managers; (2) provides cybersecurity support to components, and (3) provides oversight of component cybersecurity activities and managers.

To do so, GAO analyzed department policies, processes, and documentation. It also reviewed federal guidance and GAO and IG reports, and interviewed cognizant officials.

What GAO Recommends

GAO is making three recommendations to DOT to use annual reviews to address prior IG cybersecurity recommendations in areas such as training; ensure that senior managers' performance plans include cybersecurity-related expectations; and ensure that the DOT CIO be involved in evaluating component CIOs' performance. DOT concurred with the recommendations.

View GAO-23-106031. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

What GAO Found

Consistent with federal guidance, U.S. Department of Transportation (DOT) policy documents cybersecurity roles and responsibilities for senior officials. The policy also describes roles and responsibilities for senior managers at the nine component mission-oriented operating administrations (see figure).

Department of Transportation (DOT) Mission-Oriented Operating Administrations

Source: DOT, images: ipopba/stock.adobe.com, davooda/stock.adobe.com, EvrenKalinbacak/stock.adobe.com. | GAO-23-106031

Text for Department of Transportation (DOT) Mission-Oriented Operating Administrations

- Federal Aviation Administration
- Federal Highway Administration
- Federal Motor Carrier Safety Administration
- Federal Railroad Administration
- Federal Transit Administration
- Maritime Administration
- National Highway Traffic Safety Administration
- Pipeline and Hazardous Materials Safety Administration
- Great Lakes St. Lawrence Seaway Development Corporation

Source: DOT, images: ipopba/stock.adobe.com, davooda/stock.adobe.com, EvrenKalinbacak/stock.adobe.com. | GAO-23-106031

DOT's Office of the Chief Information Officer (CIO) regularly communicates with component agencies by sharing information through daily cyber operations meetings and periodic informational emails. Further, component agency managers stated that the office provides access to cybersecurity tools for incident and vulnerability management and other technical assistance. DOT also supported managers by providing cybersecurity role-based training. However, the DOT Inspector General (IG) reported deficiencies in the clarity of training requirements, such as the required number of hours, and the monitoring of training completion. The IG's 2019 and 2021 recommendations to address these deficiencies are not yet implemented.

To provide oversight, DOT policy requires annual reviews of component agency cybersecurity programs. However, the reviews have not been effective in taking

needed actions to implement the 63 unresolved cybersecurity recommendations as reported by the IG in a September 2022 report. Using the reviews to address the recommendations could improve the department's cybersecurity program.

To assess managers' performance, DOT established performance plans for its component agency senior IT managers. However, while DOT's strategic plan identified cybersecurity as an organizational objective, 15 of 18 managers' performance plans did not include cybersecurity-related expectations. Further, the department CIO did not always participate in evaluating the performance of component agency CIOs. This is inconsistent with department regulations and results in less assurance that component agencies are aligned with the department in carrying out cybersecurity-related responsibilities.

Contents

Abbreviations

CIO	Chief Information Officer
CISO	Chief Information Security Officer
DOT	Department of Transportation
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
NIST	National Institute of Standards and Technology
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

May 15, 2023

The Honorable Maria Cantwell
Chair
The Honorable Ted Cruz
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Sam Graves
Chair
The Honorable Rick Larsen
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Federal agencies are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. However, the IT systems supporting federal agencies and our nation's critical infrastructures are at risk.

Information and systems are subject to serious threats that can have adverse impacts on organizational operations and assets, individuals, other organizations, and the nation. These threats can include purposeful attacks, environmental disruptions, and human and machine errors, and may result in harm to the national and economic security interests of the United States.

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Therefore, it is imperative for agencies to clearly define cybersecurity-related roles and responsibilities and effectively oversee their cybersecurity programs in order to manage the risks associated with the operation and use of information systems.

In recognition of the growing threats to federal information systems, we have designated information security as a government-wide high-risk area since 1997. In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded the information security high-risk area in 2015 to include protecting the privacy of personally identifiable information. We and agency inspectors general have made numerous recommendations to address persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, and inappropriate disclosure.

The Infrastructure Investment and Jobs Act includes a provision for us to review the cybersecurity roles and responsibilities of senior IT officials at the Department of Transportation (DOT) and the extent to which they support and oversee senior IT managers at the DOT operating administrations (OA).[1] Our specific objectives for this review were to determine the extent to which DOT (1) has defined cybersecurity roles, responsibilities, and reporting relationships for department and component agency senior officials and managers; (2) provides cybersecurity support to components; and (3) provides oversight of component cybersecurity activities and managers.

Our scope was DOT Office of the Chief Information Officer (OCIO) and its senior IT officials, and the department's nine mission-oriented operating administrations and their senior IT managers.[2] Specifically, for DOT OCIO senior IT officials, we focused on the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). At the component agencies, we focused on CIO and CISO equivalent positions at the operating administrations. In this report, we refer to these equivalent positions collectively as senior IT managers.

[1]Pub. L. No. 117-58, § 25022(c), 135 Stat. 429, 878-79 (Nov. 15, 2021), 49 U.S.C. § 301 note.

[2]DOT consists of nine mission-oriented OAs: the Federal Aviation Administration, Federal Highway Administration, Federal Motor Carrier Safety Administration, Federal Railroad Administration, Federal Transit Administration, Maritime Administration, National Highway Traffic Safety Administration, Pipeline and Hazardous Materials Safety Administration, and the Great Lakes St. Lawrence Seaway Development Corporation. The DOT Office of the Secretary and Office of Inspector General are also considered OAs, but we did not include them in our scope because they are not mission-oriented agencies. OAs are DOT component agencies. 49 U.S.C. § 301 note.

To address the first objective, we obtained DOT's cybersecurity policies and procedures. We reviewed them to determine whether DOT had defined cybersecurity-related roles and responsibilities for departmental senior IT officials and OA senior IT managers. We compared them to guidance from the National Institute of Standards and Technology (NIST).[3] Additionally, we reviewed DOT OCIO organization charts and documentation of quarterly Federal Information Security Modernization Act of 2014 (FISMA) metrics from the OAs.[4]

To address the second objective, we reviewed policies related to support that the department provides to OAs, including establishing the need for cybersecurity information sharing and role-based training and compared it to federal guidance.[5] Additionally, we reviewed documentation and interviewed agency officials regarding cybersecurity-related resources that OCIO provides to the OAs. We also reviewed documentation of daily cyber operations meetings, periodic informational emails, and role-based training opportunities provided by the department. We further reviewed prior year DOT Office of Inspector General (OIG) reports for findings and prior recommendations relating to role-based training, and also interviewed OIG officials.[6]

In addition, we reviewed datasets describing the role-based training taken by OA senior IT managers in fiscal year 2022 and the dates that they completed the training. To assess the reliability of the data, we examined the datasets for inconsistencies between similar data records and

[3]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[4]Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (2014). FISMA 2014 largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to the other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[5]For example, see National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: March 2011).

[6]For example, see 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*, Report QC2022042 (Washington, D.C.: Sept. 28, 2022).

interviewed DOT OCIO officials. As discussed in this report, we found that the data were not fully reliable for our purposes.

To address the third objective, we considered federal guidance related to cybersecurity oversight and performance management.[7] We reviewed documentation of IT program reviews. We compared the documentation to DOT policy to determine whether the reviews addressed ensuring that OIG findings and recommendations from prior year FISMA audit reports are resolved. We also reviewed performance plans for the OA senior IT managers to identify the extent to which they described cybersecurity-related performance expectations. Further, we interviewed officials from DOT's Office of Human Resources to understand the performance appraisal process.

For each of the three objectives, we interviewed OCIO senior IT officials. We also interviewed the 18 OA senior IT managers individually in structured interviews. We analyzed their responses to identify common themes and trends relevant to our objectives. For more information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from May 2022 to May 2023 in accordance with generally accepted government auditing standards. 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.

Background

The DOT has the critical responsibility of delivering the world's leading transportation system, serving the American people and economy through the safe, efficient, sustainable, and equitable movement of people and goods. To do so, the department relies on around 55,000 permanent and temporary employees across 11 OAs. These administrations consist of nine mission-oriented OAs, the Office of the

[7]For example, see Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015); GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014); and GAO, *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*, GAO-03-488 (Washington, D.C.: March 2003).

Inspector General, and the Office of the Secretary of Transportation, which consists of the department's leadership headed by the Secretary of Transportation. Each individual administration is headed by a political appointee and has its own missions, goals, and responsibilities, which are achieved through various activities related to a specific transportation mode (e.g., air, rail, public transit, highways, etc.). See Table 1 for a list of the nine mission-oriented OAs and their functions.

Table 1: Department of Transportation's (DOT) Mission-Oriented Operating Administrations and Their Functions

Operating administrations	Function
Federal Aviation Administration	Oversees the safety of civil aviation through the issuance and enforcement of regulations and standards related to (1) the manufacture, operation, certification, and maintenance of aircrafts; (2) the certification of the aviation workforce; and (3) the maintenance and operations of airports.
Federal Highway Administration	Coordinates highway transportation programs through the Federal-Aid Highway Program, which provides federal financial assistance to states to construct and improve highways, roads, and bridges, and to improve the safety of public roads.
Federal Motor Carrier Safety Administration	Enforces safety and hazardous materials regulations on commercial motor vehicles (e.g., trucks for moving freight and household goods, and buses); improves commercial motor vehicle technologies and safety information systems; and increases awareness of the importance of safely operating commercial motor vehicles.
Federal Railroad Administration	Develops and monitors railroad compliance with federally mandated safety standards on track maintenance, inspection standards, and operating practices; and administers federal grant funds for passenger and freight rail infrastructure and services (including Amtrak), safety improvements, and congestion relief programs.
Federal Transit Administration	Promotes the development, improvement, and safety of public transportation systems, which include buses, rail, trolleys, and ferries, through a variety of federal grant programs to local transit agencies. Oversees these grants and evaluates whether grantees adhere to federal standards.
Maritime Administration	Fosters, promotes, and develops the maritime industry of the United States by supporting the technical aspects of America's maritime transportation infrastructure, including ships and shipping, port and vessel operations, national security, the environment, and safety. Promotes the use of waterborne transportation and ensures infrastructure integrates with other methods of transport. Maintains a fleet of cargo ships in reserve to provide sea-lift during war and national emergencies.
National Highway Traffic Safety Administration	Sets and enforces safety performance standards for motor vehicles and equipment and provides grants to state and local governments for conducting local highway safety programs. Investigates safety defects in motor vehicles, sets and enforces fuel economy standards, helps states and local communities address impaired driving, promotes the use of safety technologies, and conducts research on driver behavior and traffic safety, among other activities.
Pipeline and Hazardous Materials Safety Administration	Oversees the safe transportation of oil, gas, and other hazardous materials by all transportation modes, including pipelines, through the development and enforcement of regulations and standards, education, research, and assistance to the emergency response community. Oversees the safety of the nation's oil and gas pipeline network by inspecting pipelines, collecting and analyzing data, and investigating accidents to identify potential safety improvements.

Operating administrations	Function
Great Lakes St. Lawrence Seaway Development Corporation	Works with the Canadian St. Lawrence Seaway Management Corporation to oversee operations for commercial and noncommercial vessels on the Great Lakes and St. Lawrence Seaway; coordinates with Canadian authorities on operational issues such as traffic management, navigation aids, safety, and environmental programs.[a]

Source: DOT. | GAO-23-106031

[a]The Great Lakes St. Lawrence Seaway Development Corporation is a wholly owned government corporation within DOT.

The Office of the Secretary oversees the formulation of national transportation policy, promotes intermodal transportation, and coordinates the activities of each mission-oriented administration.[8] Within the Office of the Secretary is the CIO, who leads OCIO and serves as the principal advisor to the Secretary of Transportation and operating administrations on IT matters.

The CIO is responsible for all matters involving IT, including cybersecurity, privacy, and records management, among other things. The CIO is the authoritative source of departmental policy and associated implementation procedures for the management and execution of all resources within DOT's $3.5 billion annual IT portfolio. These resources include, but are not limited to, information systems operating within and outside of the department's internal network. Within OCIO, the CISO oversees the department's information security program and also serves as a senior advisor to the CIO and other senior leadership on cybersecurity strategy and policy. OA CIOs and CISOs, or their equivalents, oversee cybersecurity at each of the mission-oriented OAs.[9]

DOT Relies on Information Systems and Networks to Carry Out Its Mission

The Department relies on about 450 IT systems to carry out its mission. DOT OCIO provides OAs, except for the Federal Aviation Administration,

[8]Intermodal transportation refers to the movement of freight or passengers using more than one mode of transportation to complete a journey, such as by sea, rail, or truck.

[9]OA CIO and CISO equivalents have varying job titles. Of the nine OA CIO equivalents, three were CIOs, three were Chief Technology Officers, two were Associate Administrators, and one was a Budget Officer. Similarly, of the nine OA CISO equivalents, two were CISOs, six were Information Systems Security Managers, and one was an IT Specialist. In this report, they will be referred to as CIO equivalents, CISO equivalents, and collectively as OA senior IT managers.

with IT services within its common operating environment.[10] These services include, but are not limited to, network, email, and messaging services; desktop computer management; data storage; and a centralized environment for applications.

Federal Law and Guidance Establish a Framework for Managing Federal Systems and Protecting Them from Cybersecurity Threats

The Federal Information Technology Acquisition Reform Act (FITARA) was enacted in December 2014 to improve certain federal agencies' acquisitions of IT and better enable Congress to monitor agencies' efforts and hold them accountable for reducing duplication and achieving cost savings.[11] FITARA establishes specific requirements related to agency CIO authority enhancements including a role in the approval of bureau CIOs and oversight processes related to IT.[12] After FITARA's enactment, the Office of Management and Budget published guidance to agencies to ensure that the act is applied consistently government-wide in a way that is both workable and effective.[13]

[10]DOT's common operating environment network provides email management, computer infrastructure, internet access, and other IT services to users in all of DOT's operating administrations except the Federal Aviation Administration.

[11]The Federal Information Technology Acquisition Reform Act is the popular name for the federal IT acquisition reform provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014). The Department of Transportation is one of 24 federal agencies that are subject to the requirements in FITARA. FITARA references the list of 24 federal agencies in 31 U.S.C. § 901(b)(1) (Chief Financial Officers Act of 1990), which includes DOT.

[12]For the purposes of this report, bureau is defined as one of the department's nine mission-oriented operating administrations.

[13]Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015). This guidance describes how covered agencies are to implement the requirements of the law in conjunction with prior IT laws through the use of management controls, including controls related to the development of IT budgets. The guidance identifies a number of actions that agencies are to take to establish a basic set of roles and responsibilities for CIOs and other senior agency officials.

Additionally, several federal laws and guidance provide a framework for assisting agencies with protecting federal systems and managing cybersecurity threats and risks. Key examples include:

- The Federal Information Security Modernization Act of 2014 (FISMA) establishes requirements for federal agencies, including DOT, to address cybersecurity within their operating environment.[14] The act provides a comprehensive framework for ensuring effective controls over information resources that support federal operations and assets, among other things.
- The National Institute of Standards and Technology (NIST) has published guidance for an integrated, organization-wide program for managing information security risk.[15] According to NIST, the guidance provides a structured, yet flexible approach for managing risk that is intentionally broad-based. NIST provides specific details for assessing, responding to, and monitoring risk on an ongoing basis provided by its other supporting security standards and guidelines.
- In addition, NIST has published a catalog of security and privacy controls for federal information systems and organizations.[16] The catalog provides a process for selecting controls to protect organizational operations, assets, individuals, other organizations, and the nation from a diverse set of threats.

OIG's Auditor Reported the Department's Information Security Program as Ineffective

In its fiscal year 2022 FISMA audit report, the DOT IG's independent auditor stated that the department's overall information security program

[14]Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (2014). FISMA 2014 largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to the other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[15]National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: March 2011).

[16]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 revision 5 (Gaithersburg, MD: September 2020).

was ineffective.[17] The independent auditor identified deficiencies related to risk management, supply chain risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning.[18] The auditor reported that many of these weaknesses could be attributed to inconsistent enforcement of an agency-wide information security program, ineffective communication between the department and the OAs, and the department's lack of progress in remediating weaknesses identified in prior years. The report included eight new recommendations intended to help the department address challenges in its development of a mature and effective information security program. Further, the auditor noted that the department had not yet implemented 63 prior recommendations from previous FISMA audits.

DOT Has Defined Cybersecurity Roles and Responsibilities and Documented Reporting Relationships

DOT has documented cybersecurity roles and responsibilities for department-level senior IT officials and OA senior IT managers in departmental policy. Additionally, the department has established cybersecurity-related reporting relationships between department officials and OA managers.

[17]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*, Report QC2022042 (Washington, D.C.: Sept. 28, 2022). According to the department's Office of Inspector General, since 2019, it has contracted with an independent auditor to conduct the annual FISMA audit. Prior to 2019, the Office of Inspector General itself conducted the audits.

[18]In December 2020, we reported that DOT had not assessed skill gaps in cybersecurity positions. We recommended that DOT assess skill gaps in cybersecurity positions, and other key occupations that are involved in overseeing the safety of automated technologies. DOT agreed with this recommendation, and has taken some steps to develop a tool to assess these skill gaps. However, DOT has not yet finalized or implemented the tool. See GAO, *Automated Technologies: DOT Should Take Steps to Ensure Its Workforce Has Skills Needed to Oversee Safety*, GAO-21-197 (Washington, D.C.: December 2020).

DOT Defined Cybersecurity Roles and Responsibilities for Senior IT Leaders

NIST guidance states that an effective cybersecurity program should be based, in part, on the implementation of a program plan that identifies and assigns roles and responsibilities for implementing the plan.[19] Additional NIST guidance identifies the roles and responsibilities for CIOs and CISOs within agencies.[20] CIOs should be responsible for

- overseeing organization-wide information security programs to ensure adequate security of systems;
- ensuring that technology is managed in a manner consistent with all laws and other regulations;
- overseeing personnel with significant information security responsibilities;
- assisting senior organizational officials regarding their security responsibilities; and
- designating a senior information security officer.

In addition, CISOs should be responsible for

- carrying out the CIO's responsibilities under FISMA;[21]
- coordinating, developing, implementing and maintaining an organization-wide information security program; and
- serving as the liaison for the CIO to the organization's authorizing officials, system owners, and information system security officers, among others.

DOT has documented roles and responsibilities for senior officials and OA senior managers in its departmental cybersecurity policy consistent with NIST guidance. Specifically, the policy lays out its cybersecurity program, including roles and responsibilities for departmental and OA senior officials. The policy assigns the departmental CIO responsibility for

- managing the departmental cybersecurity program;

[19]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[20]National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: March 2011).

[21]These responsibilities are set forth in 44 U.S.C. § 3554.

- ensuring compliance with federal regulations and FISMA IT security program implementation requirements;
- assisting agency leaders and other personnel to ensure security policies and procedures are followed; and
- appointing the departmental CISO to fulfill the responsibilities of the CIO in maintaining the cybersecurity program.

In addition, the departmental CISO is responsible for

- fulfilling the role of the CIO as it relates to FISMA, including preparation of monthly, quarterly, and annual FISMA reports;
- providing management leadership in cybersecurity policy and guidance;
- assisting and advising the CIO in the development, documentation, and implementation of the cybersecurity program; and
- serving as the primary liaison between the departmental CIO and OA CIOs, information systems security managers, and others.

The policy also defines roles and responsibilities for OA senior IT managers, including OA CIO equivalents. Specifically, the policy states that such individuals are responsible for, among other things,

- managing the cybersecurity program for their administration and advising the OA head on significant issues related to the cybersecurity program;
- ensuring that security assessment and authorization of OA information systems is accomplished in accordance with DOT policy and NIST guidance; and
- reporting OA cybersecurity-related information to the departmental CIO to meet the department's cybersecurity requirements.

Moreover, the OA CISO equivalents are responsible for, among other things,

- overseeing the OA's cybersecurity program;
- ensuring that the OA CIO and DOT CISO are kept apprised of all pertinent matters involving the security of information systems;
- managing cybersecurity resources including oversight and review of security requirements in funding documents; and
- serving as the primary liaison for the OA CIO to the administration's authorizing officials, information system owners, and others with cybersecurity responsibilities.

Further, 16 of the 18 senior IT managers at the operating administrations stated that their roles and responsibilities were well documented. Specifically, one official identified the value of the descriptive nature of

component level positions within the policy as useful. Another stated that the information contained in the policy was sufficient and clarified roles and responsibilities. For the remaining two managers, they described the documented roles and responsibilities as workable. For example, one suggested that DOT may need to review the policy since several years had elapsed since the last update, and the other suggested possible updates to add more specificity of roles and responsibilities for their operating administration.

DOT Documented Cybersecurity-Related Reporting Relationships with OA Senior IT Managers

DOT's cybersecurity policy also identifies reporting relationships between DOT senior IT officials and OA senior IT managers. Specifically, the policy gives the department-level CIO responsibility for working closely with OA senior IT managers to ensure the proper implementation of the cybersecurity program. The department-level CISO also has responsibility for serving as the primary liaison for OA senior IT managers. At the operating administration level, the policy requires OA CIO equivalents to report cybersecurity-related information to the department's CIO. Further, CISO equivalents at the OAs are required to keep the CIO and the department-level CISO apprised of all relevant cybersecurity matters within their operating administration.

DOT Provided Cybersecurity Support to OA Senior IT Managers, but Role-Based Training Requirements Were Unclear

DOT senior IT officials shared cybersecurity information with OA senior IT managers through regular meetings and informational emails. These officials also provided OA senior IT managers with cybersecurity-related resources, such as cybersecurity tools, and required them to take cybersecurity-related role-based training annually. However, the role-based training data were inconsistent. Additionally, the DOT OIG previously reported that OCIO had not sufficiently monitored the completion of role-based training or clearly defined role-based training requirements.

DOT Senior IT Officials Shared Cybersecurity Information

Given the risks that cybersecurity threats present, it is increasingly important that organizations share cyber threat information and use it to improve their security posture. Federal guidance and DOT policy establish criteria for sharing cybersecurity risk-related information within the organization. For example:

- NIST recommends that organizations establish organization-wide forums to consider all types and sources of risk, and establish effective methods for communicating and sharing risk-related information among key stakeholders internally and externally to organizations.[22]
- DOT's cybersecurity policy states that the CISO is to promote collaboration among DOT OAs in developing, promoting and maintaining IT security measures. The CISO is also responsible for fostering communication and collaboration among DOT's security stakeholders to share knowledge and better understand threats to departmental information.

DOT senior officials promoted communication of cybersecurity information with and among OA senior managers (i.e., CIO and CISO equivalents at the operating administrations) in accordance with federal guidance and departmental policy. Specifically, they shared information through daily cyber operations meetings and periodic informational emails.

- **Daily cyber operations meetings.** The department's OCIO and cybersecurity leaders from each of the OAs meet daily to discuss cybersecurity topics. According to an OA senior manager, the meetings initially started in December 2021 as a response to a system vulnerability that existed at the time.[23] OCIO officials stated that the meetings provide a mechanism for the department to discuss, present, and prioritize cybersecurity activities on a daily basis. According to the officials, the activities discussed included

[22]National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: March 2011).

[23]In December 2021, a vulnerability was discovered in the Apache Log4j framework, which is a type of cyber security logging software used in websites and web applications across the world. The vulnerability, if left unmitigated, could allow malicious individuals to break into online-based systems, including cloud services and applications, to compromise data.

vulnerability management, configuration management, and a briefing of new threats from the security operations center.

The OA senior managers generally found the meetings useful. Of the 18 managers

- twelve indicated that they found the meetings helpful in providing situational awareness on cybersecurity matters throughout the department;
- eight also noted that the meetings helped to foster cooperation and collaboration between the operating administrations; and
- three added that the meetings helped with ensuring that their cybersecurity efforts are aligned with departmental goals.

However, one individual stated that the meetings were repetitive and could be held once or twice per week instead of every day.

- **Periodic informational emails.** Nine of the 19 OA senior managers told us that OCIO provides periodic emails that include updates on cybersecurity matters, among other things. Cybersecurity-related information communicated in the periodic emails includes, for example, updates on risk and vulnerability assessments, updates on hiring efforts, policy updates, cybersecurity training opportunities, and assistance available to OAs.

Nevertheless, although these efforts are in place, the DOT Office of Inspector General has reported that DOT faces significant challenges in implementing its cybersecurity program. According to the OIG, these challenges are due, at least in part, to ineffective communication between the department and the OAs. OIG officials stated that the communication problems stemmed from DOT not having a full-time CISO in place. During the course of our review, in August 2022, DOT hired a full-time CISO.[24]

DOT Provided OAs Access to Cybersecurity Tools and Other Resources

Fifteen of the 18 OA senior IT managers stated that OCIO provided the administrations with access to cybersecurity tools. OCIO officials explained that these tools included incident management, vulnerability management, and Web application testing tools, among others. The

[24]According to DOT OCIO officials, the CISO served in an acting role beginning in November 2020. However, these officials stated that although in an acting role, the duties of the acting CISO were primarily focused on cybersecurity.

remaining three managers were unsure whether the department provided cybersecurity tools or had no response.

Eleven of the 18 OA senior IT managers also stated that OCIO provided departmental personnel to assist with cybersecurity-related matters. For example, one manager stated that the OCIO cybersecurity and information protection group has several cybersecurity engineers that provide a great deal of support through reports, vulnerability identification, risk management, cyber tool administration, and report interpretation. Another manager stated that department personnel assisted in planning for implementing two-factor authentication on the OA's legacy systems. The remaining seven managers stated that OCIO had not been involved with providing personnel for cybersecurity assistance at their OAs.

DOT Provided Cybersecurity Role-Based Training, but Tracking and Requirements Were Unclear

NIST recommends that agencies provide role-based security and privacy training to personnel with significant cybersecurity responsibilities, including senior leaders or management officials.[25] Additionally, DOT policy requires that employees with significant cybersecurity responsibilities, such as OA senior IT managers, complete role-based cybersecurity training on an annual basis.

To facilitate annual role-based training completion, DOT provides various training opportunities. For example, the department holds a cybersecurity symposium annually, which is comprised of keynote speakers and role-oriented sessions. In addition, the department provides role-based, online courses through its electronic learning management system and forwards external agency training opportunities to managers.

However, the department provided data on role-based training completion dates that was inconsistent. DOT initially provided a dataset containing various training completion dates for the 14 OA senior IT managers for fiscal year 2022.[26] Subsequently, the department provided another

[25]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53 revision 5 (Gaithersburg, MD: September 2020).

[26]The department's fiscal year 2022 started October 1, 2021 and ended September 30, 2022. 14 senior IT managers were in their current positions as of October 1, 2021, and required to complete role-based training in fiscal year 2022. In fiscal year 2022, the department's training reporting cycle started October 1, 2021 and ended August 31, 2022.

dataset, also for fiscal year 2022, with different dates for 12 of the 14 managers.

According to an OCIO official, the department aggregates data from several training environments and uses multiple methods to monitor training completion, including manually in a spreadsheet. The official noted that the department has faced challenges with completion dates because multiple data sources exist. The official added that the department plans to implement a more centralized system for tracking role-based training in the near future.

The Inspector General's independent auditor made a recommendation related to the oversight and monitoring of training completion. In 2021, the independent auditor recommended that the department develop and implement a process for integrated and centralized monitoring of training completion. DOT concurred with the recommendation, but according to the fiscal year 2022 FISMA report, the department had not yet implemented it.

Additionally, OA senior IT managers were unsure of the role-based training requirements. For example, the 18 OA senior IT managers gave inconsistent answers indicating confusion about the training requirements. Specifically:

- eight acknowledged the role-based training requirement, but did not mention a required number of hours;
- four indicated the training requirement was equal to one hour;
- two acknowledged the training requirement, but were unsure of the required number of hours;
- one stated the training requirement was not based on time;
- one noted that they were unsure of training requirements;
- one indicated there were no role-based training requirements; and
- one did not indicate whether they were or were not aware of training requirements.

In 2019, the Inspector General recommended that the department update role-based training guidance to clearly define requirements and the department concurred with it. According to the Inspector General's report, as a result of unclear requirements, most administrations did not provide employees' hours of training, and therefore, the Inspector General could not determine if employees met training requirements. According to the fiscal year 2022 FISMA report, the department had not yet implemented this recommendation.

Because of the open Inspector General's recommendations, we are not making additional recommendations related to tracking role-based training completion and updating requirements.

DOT Held IT Program Reviews and Developed Manager Performance Plans but Lacked Sufficient Oversight

DOT can hold senior IT managers accountable through IT program reviews and performance management appraisals. DOT held IT program reviews with OAs that covered several areas of IT management, including cybersecurity. However, the reviews did not include efforts to address unresolved OIG FISMA audit recommendations. In addition, DOT established performance plans for its OA senior IT managers, but the performance plans did not always include expectations related to the manager's cybersecurity responsibilities. Further, the DOT CIO did not always provide input for OA CIO equivalent's performance appraisals.

DOT Conducted IT Program Reviews, but These Reviews Did Not Address Unresolved OIG FISMA Recommendations

DOT's security authorization and continuous monitoring policy states that the DOT CISO is to perform program performance oversight and analysis reviews of OA cybersecurity programs annually. According to the policy, these reviews are to include several elements of a cybersecurity risk management program, such as system authorizations, system contingency planning and testing, remediating system vulnerabilities, and annual security and privacy training requirements. The reviews are also to address ensuring that DOT OIG findings and recommendations from prior year FISMA audit reports are resolved.

OCIO officials stated that, beginning in fiscal year 2022, the program performance oversight and analysis reviews had been combined into annual IT program reviews for each OA. These reviews covered multiple areas of IT management, including funding, system inventory, major IT investments, and IT workforce, in addition to cybersecurity.

As of September 1, 2022, OCIO had held IT program reviews with eight of the nine mission-oriented OAs. These reviews covered various aspects

of cybersecurity, including system multifactor authentication compliance,[27] system authorization status,[28] contingency planning and testing, and plans of action and milestones.[29] However, the agendas and discussion materials for the reviews did not address resolution of recommendations from prior year OIG FISMA audits. As of September 2022, 63 of these recommendations remained unresolved, with at least one dating back to 2011.[30] An OCIO official stated that the department planned to include discussions of unresolved OIG FISMA recommendations in these reviews in the future. Without leveraging these reviews to help address unresolved recommendations identified in prior year DOT OIG FISMA reports, DOT will likely continue to face challenges in ensuring that weaknesses in its cybersecurity program are remediated.

DOT Did Not Always Establish Cybersecurity Expectations for, or Monitor Performance of, OA Senior IT Managers

The Office of Management and Budget's Federal Information Technology Acquisition Reform Act (FITARA) implementation guidance states that covered agencies are to establish an agency-wide critical element (or

[27]Multifactor authentication involves using two or more factors to achieve authentication. Factors include something you know (password or personal identification number), something you have (cryptographic identification device or token), or something you are (biometric).

[28]An authorization to operate is issued when a system's authorizing official reviews the system authorization package and deems the risks associated with the system acceptable. The security authorization package documents the results of the security control assessment and provides the authorizing official with essential information to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

[29]A plan of action and milestones identifies tasks needing to be accomplished to address an identified cybersecurity vulnerability. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

[30]The DOT OIG's independent auditor made eight new recommendations in its fiscal year 2022 FISMA report.

elements)[31] for the evaluation of component CIOs.[32] In addition, GAO's key practices for effective performance management collectively create a clear linkage—"line of sight"—between individual performance and organizational success.[33] Among other things, these practices state that organizations should align individual performance expectations with organizational goals.

Moreover, the Office of Management and Budget guidance also states that the CIO should provide input to the rating official for at least all key bureau CIOs at the time of the initial summary rating and for any required progress reviews. DOT regulations also require the department CIO to participate in the performance reviews of the OA CIOs.[34] Further, GAO's *Standards for Internal Control in the Federal Government* state that management should evaluate performance and hold individuals accountable for their internal control responsibilities.

DOT established performance plans for its OA senior IT managers in order to evaluate their individual performance. However, although DOT identified cybersecurity risk as one of its organizational objectives in its strategic plan, the critical elements in the performance plans did not always include expectations that were aligned with this objective. Specifically:[35]

- Of the nine OA senior IT managers that were CIO equivalents, the performance plans for eight did not include cybersecurity-related expectations. Additionally, while the remaining plan included a statement that the individual was responsible for strategic leadership

[31]The Office of Personnel Management defines a critical element as a work assignment or responsibility of such importance that unacceptable performance on that element would result in a determination that the employee's overall performance is unacceptable. 5 C.F.R. § 430.203. Government-wide regulations require employees have at least one critical element in their performance plans. 5 C.F.R. § 430.206(b)(4). Critical elements must address performance at the individual level only.

[32]Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

[33]GAO-03-488.

[34]49 C.F.R. § 1.48.

[35]According to the Office of Personnel Management, employee performance plans are all of the written, or otherwise recorded, performance elements that set forth expected performance. A plan must include all critical and non-critical elements and their performance standards.

for the secure deployment of IT resources, it did not include detailed cybersecurity-related expectations that could be used to evaluate an individual's performance.

- Of the nine OA senior IT managers that were CISO equivalents, the performance plans for three described cybersecurity-related performance expectations that could be used to evaluate an individual's performance. Although the plans for three others included statements indicating that the individuals had cybersecurity responsibilities, the plans did not include detailed cybersecurity-related performance expectations that could be used to evaluate performance. The plans for the remaining three CISO equivalents did not include cybersecurity-related performance expectations at all.

DOT OCIO officials pointed out that there is no federal requirement for DOT to establish separate cybersecurity performance expectations outside of the standard human resources performance program. However, our key practices for effective performance management state that organizations should align individual performance expectations with organizational goals. Departmental policy does not require that OA senior IT managers' performance plans include cybersecurity-related expectations. The officials stated that any effort to develop and implement such a policy would require working with the department's office of human resources, because OCIO does not have the authority to issue human resources-related policies alone. By not including cybersecurity-related expectations in performance plans, DOT has less assurance that it can effectively monitor the individual performance of OA senior IT managers or hold them accountable for carrying out their individual cybersecurity-related responsibilities.

In addition, the DOT CIO did not always participate in the performance reviews of the OA CIO equivalents. Specifically, the CIO did not always provide input for OA CIO equivalent's performance appraisals. For example, in November 2022, an OCIO official provided concurrence on the performance appraisals for four of the nine OA CIO equivalents. However, OCIO did not provide documentation of concurrence for the other five. The department issued guidance in 2008 regarding having input for these appraisals, but subsequent guidance for IT management at the department did not address performance appraisals. Without input from the department CIO, DOT has less assurance that OA CIO equivalents are held accountable for meeting cybersecurity-related organizational goals.

Conclusions

Given the risks that cybersecurity threats present, it is increasingly important that organizations define cybersecurity roles and responsibilities and share cyber threat information to improve their security posture. Establishing and maintaining effective communications between the OA senior IT managers and the department is critical for DOT in addressing the longstanding weaknesses in the implementation of its cybersecurity program.

In addition, ensuring that longstanding IG recommendations are addressed is essential for the department in reducing the risk to its information systems. However, although DOT conducted IT program reviews with its OAs, the department did not use these reviews to help address the recommendations. Leveraging these reviews to address recommendations that have not yet been implemented could help improve the department's cybersecurity program.

Further, establishing cybersecurity-related performance expectations for OA senior IT managers and overseeing the performance of OA CIO equivalents helps to hold managers accountable for carrying out their cybersecurity responsibilities effectively. Although DOT established performance plans for these managers, the plans did not always include cybersecurity-related expectations. Additionally, the CIO did not always participate in the performance reviews of OA CIO equivalents. As a result, DOT has less assurance that operating administrations are aligned with the department in carrying out cybersecurity-related responsibilities.

Recommendations for Executive Action

We are making the following three recommendations to DOT:

The Secretary of Transportation should direct the DOT CIO to leverage its IT program reviews to address recommendations that have not yet been implemented from prior year DOT OIG FISMA reports. (Recommendation 1)

The Secretary of Transportation should direct the DOT CIO to collaborate with human resources officials to develop and implement a policy requiring that OA senior IT managers' performance plans include cybersecurity-related performance expectations. (Recommendation 2)

The Secretary of Transportation should ensure that the DOT CIO participates in the performance reviews of OA CIO equivalents. (Recommendation 3)

Agency Comments

We provided a draft of this report to DOT for review and comment. In written comments, reprinted in appendix II, DOT concurred with our three recommendations. The department further highlighted actions DOT has taken to prioritize cybersecurity, including holding daily cybersecurity meetings with OA IT and cybersecurity officials, initiating IT program reviews with OA IT and budget officials, and prioritizing the recruitment and retention of cybersecurity talent for its workforce. DOT also provided technical comments, which we have incorporated in the report as appropriate.

We are sending copies of this report to appropriate congressional committees, the Secretary of Transportation, the DOT Chief Information Officer, the DOT Inspector General, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Jennifer R. Franks
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

The objectives for this review were to determine the extent to which the Department of Transportation (DOT) (1) has defined cybersecurity roles, responsibilities, and reporting relationships for department and component agency senior IT officials and managers; (2) provides cybersecurity support to components; and (3) provides oversight of component cybersecurity activities and managers.

For the scope of this report, we selected the nine mission-oriented operating administrations (OA):[1]

- Federal Aviation Administration
- Federal Highway Administration
- Federal Motor Carrier Safety Administration
- Federal Railroad Administration
- Federal Transit Administration
- Maritime Administration
- National Highway Traffic Safety Administration
- Pipeline and Hazardous Materials Safety Administration
- Great Lakes St. Lawrence Seaway Development Corporation

We considered the DOT Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to be DOT senior IT officials. Additionally, we considered the CIO and CISO equivalents at each of the nine mission-oriented OAs to be senior IT managers.[2]

To address the first objective, we obtained DOT's cybersecurity policies and procedures. We reviewed them to determine whether DOT had defined cybersecurity-related roles and responsibilities for departmental

[1]DOT consists of 11 operating administrations. The DOT Office of the Secretary and Office of Inspector General are considered operating administrations, but we did not include them in our scope because they are not mission-oriented agencies.

[2]Operating administration CIO and CISO equivalents have varying job titles. Of the nine CIO equivalents, three had the title of CIO, three had the title of Chief Technology Officer, two were Associate Administrators, and one was a Budget Officer. Similarly, of the nine CISO equivalents, two had the title of CISO, six were Information Systems Security Managers, and one was an IT Specialist.

senior IT officials and OA senior IT managers. We compared them to guidance from the National Institute of Standards and Technology (NIST).[3] Additionally, we reviewed DOT Office of the Chief Information Officer (OCIO) organization charts and documentation of quarterly Federal Information Security Modernization Act (FISMA) metrics from the OAs.[4] We reviewed these in order to determine the extent to which DOT had established reporting relationships with respect to cybersecurity.

We also determined that the control environment component of internal control was significant to this objective, along with the underlying principle that management should assign responsibility and delegate authority to achieve the entity's objectives.[5] As previously noted, we assessed DOT policies and procedures and reviewed organizational charts to determine whether DOT had established cybersecurity roles and responsibilities for departmental senior IT officials and OA senior IT managers.

To address the second objective, we reviewed policies related to support that the department provides to OAs, including establishing the need for cybersecurity information sharing and role-based training and compared it to federal guidance.[6] Additionally, we reviewed documentation and interviewed agency officials regarding cybersecurity-related resources that OCIO provides to the OAs. We also reviewed documentation of daily cyber operations meetings and periodic informational emails to determine how cybersecurity information is shared between OCIO and the OAs. We

[3]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: September 2020).

[4]Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128 Stat. 3073 (2014). FISMA 2014 largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers to the new requirements in FISMA 2014, and to the other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[5]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[6]For example, see National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: March 2011).

compared these documents with NIST guidance[7] and DOT policies on cybersecurity information sharing.

We reviewed documentation of cybersecurity symposium offerings and other role-based training opportunities provided by the department. We also reviewed prior year DOT Office of Inspector General (OIG) reports for findings and prior recommendations relating to role-based training and interviewed OIG officials about prior communication findings.

We also reviewed datasets describing the role-based training taken by OA senior IT managers in fiscal year 2022 and the dates that they completed the training. We compared this information with NIST guidance and DOT policies on providing role-based security training to personnel with cybersecurity responsibilities. To assess the reliability of these data, we identified differences in training completion dates between two datasets we received and interviewed OCIO officials about how the data are collected and tracked. After taking these steps, we determined that the data were not fully reliable for our purposes.

Further, we also determined that the information and communication component of internal control was significant to this objective. This includes the underlying principle that management should internally communicate the necessary quality information to achieve the entity's objectives.[8] As previously noted, we reviewed documentation of cybersecurity information sharing activities to determine how cybersecurity information is shared between the departmental OCIO and the OAs. We also evaluated whether DOT used reliable data to record and track the completion of role-based cybersecurity training by OA senior IT managers.

To address the third objective, we reviewed documentation of IT program reviews. We compared the documentation to DOT policy to determine whether the reviews addressed ensuring that OIG findings and recommendations from prior year FISMA audit reports are resolved. We also reviewed DOT's strategic plan to identify whether cybersecurity is part of DOT's strategic goals. We also reviewed performance plans for

[7]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations,* Special Publication 800-53 revision 5 (Gaithersburg, MD: September 2020).

[8]GAO-14-704G.

the 18 OA senior IT managers to identify the extent to which they described cybersecurity-related performance goals. We compared these with GAO's key practices for effective performance management regarding aligning individual performance expectations with organizational goals.[9]

Finally, we interviewed officials from DOT's Office of Human Resources to understand the performance appraisal process, and interviewed DOT OCIO officials to determine whether the CIO has a role in the performance appraisal process of OA senior IT managers. We compared the information obtained through these interviews with guidance from the Office of Management and Budget[10] for the agency CIO's role in evaluating the performance of component CIOs.[11]

We also determined that the control environment component of internal control was significant to this objective, along with the underlying principle that management should evaluate performance and hold individuals accountable for their internal control responsibilities.[12] As previously noted, we reviewed the performance plans for OA senior IT managers and interviewed officials from DOT's Office of Human Resources and OCIO. We did this in order to determine how the department evaluates the performance of OA senior IT managers and holds them accountable for carrying out their cybersecurity-related responsibilities.

For each of the three objectives, we also interviewed department-level OCIO senior IT officials and the 18 CIO and CISO equivalents at the operating administrations. We also developed a set of structured interview questions for interviewing the 18 OA CIO and CISO equivalents individually. We analyzed the responses to the structured interview

[9]GAO, *Results-Oriented Cultures: Creating a Clear Linkage between Individual Performance and Organizational Success*, GAO-03-488 (Washington, D.C.: March 2003).

[10]Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies: Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

[11]The Office of Personnel Management defines a critical element as a work assignment or responsibility of such importance that unacceptable performance on that element would result in a determination the employee's overall performance is unacceptable. Government-wide regulations require employees have at least one critical element in their performance plans. Critical elements must address performance at the individual level only.

[12]GAO-14-704G.

questions to identify common themes and trends relevant to our objectives.

We conducted this performance audit from May 2022 to May 2023 in accordance with generally accepted government auditing standards. 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.

Appendix II: Comments from the Department of Transportation

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

Assistant Secretary for Administration

1200 New Jersey Avenue, S.E.
Washington, DC 20590

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

DATE: April 28, 2023

Dear Director Franks,

The mission of the Department of Transportation (DOT) is to deliver the world's leading transportation system serving the American people and economy through the safe, efficient, sustainable, and equitable movement of people and goods. This mission includes achieving cybersecurity and the protection of information in transportation systems, and coordinating with our sector risk management agency partners, industry and others to manage and mitigate cybersecurity risks within the transportation sector.

DOT continues to prioritize cybersecurity in response to the continued evolution of cyber threats, additions to federal policy such as the requirements in Executive Order 14028, *Improving the Nation's Cybersecurity*, and enhancements to agency missions and information systems. DOT initiated daily cybersecurity meetings with component Operating Administration (OA) information technology (IT) and cybersecurity officials in January 2021 to expedite the reduction of vulnerabilities and modernize technologies on DOT networks, to drive progress on encryption of data at rest and in transit, and to standardize the use of multifactor authentication on agency systems. DOT restructured its portfolio review processes in Fiscal Year 2022 and initiated IT "Deep Dive" reviews with OA IT and budget officials to improve communication and oversight and make progress on key initiatives including the hosting of new and modernized systems in FedRAMP certified commercial cloud environments. DOT has also prioritized the recruitment and retention of top cybersecurity talent for DOT's cybersecurity workforce.

Upon review of the draft report, the Department concurs with GAO's three recommendations directing the DOT Chief Information Officer to (1) leverage its IT program reviews to address recommendations that have not yet been implemented from prior year DOT Office of Inspector General Federal Information Security Management Act reports, (2) collaborate with human resources officials to develop and implement a policy requiring that OA senior IT managers' performance plans include cybersecurity-related performance expectations, and (3) ensure that the DOT CIO has a role in evaluating the performance of OA CIO equivalents. DOT will provide a detailed response to the recommendations within 180 days of the report's final issuance.

DOT appreciates the opportunity to respond to the GAO draft report. Please contact Gary Middleton, Director of Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like additional information.

Sincerely,

Philip McNamara
Assistant Secretary for Administration

Text from Appendix II: Comments from the Department of Transportation

U.S. Department of Transportation
Office of the Secretary of Transportation
Assistant Secretary for Administration
1200 New Jersey Avenue, S.E.
Washington, DC 20590

Jennifer R. Franks DATE: April 28, 2023
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office (GAO)
441 G Street NW
Washington, DC 20548

Dear Director Franks,

The mission of the Department of Transportation (DOT) is to deliver the world's leading transportation system serving the American people and economy through the safe, efficient, sustainable, and equitable movement of people and goods. This mission includes achieving cybersecurity and the protection of information in transportation systems, and coordinating with our sector risk management agency partners, industry and others to manage and mitigate cybersecurity risks within the transportation sector.

DOT continues to prioritize cybersecurity in response to the continued evolution of cyber threats, additions to federal policy such as the requirements in Executive Order 14028, Improving the Nation's Cybersecurity, and enhancements to agency missions and information systems. DOT initiated daily cybersecurity meetings with component Operating Administration (OA) information technology (IT) and cybersecurity officials in January 2021 to expedite the reduction of vulnerabilities and modernize technologies on DOT networks, to drive progress on encryption of data at rest and in transit, and to standardize the use of multifactor authentication on agency systems. DOT restructured its portfolio review processes in Fiscal Year 2022 and initiated IT "Deep Dive" reviews with OA IT and budget officials to improve communication and oversight and make progress on key initiatives including the hosting of new and modernized systems in FedRAMP certified commercial cloud environments. DOT has also prioritized the recruitment and retention of top cybersecurity talent for DOT's cybersecurity workforce.

Upon review of the draft report, the Department concurs with GAO's three recommendations directing the DOT Chief Information Officer to (1) leverage its IT program reviews to address recommendations that have not yet been implemented from prior year DOT Office of Inspector General Federal Information Security Management Act reports, (2) collaborate with human resources officials to develop and implement a policy requiring that OA senior IT managers' performance plans include cybersecurityrelated performance expectations, and (3) ensure that the DOT CIO has a role in evaluating the performance of OA CIO equivalents. DOT will provide a detailed response to the recommendations within 180 days of the report's final issuance.

DOT appreciates the opportunity to respond to the GAO draft report. Please contact Gary Middleton, Director of Audit Relations and Program Improvement, at (202) 366-6512 with any questions or if GAO would like additional information.

Sincerely,

Philip McNamara
Assistant Secretary for Administration

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer R. Franks, (404) 679-1831, franksj@gao.gov.

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (assistant director), William Cook (analyst-in-charge), Amanda Andrade, Chris Businsky, Donna Epler, Shane Homick, and AJ Yohn made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548