Strengthening DOT's Cybersecurity Program To Protect the Nation's Transportation Infrastructure

December 2, 2021
CC2022001

Statement of Kevin Dorsey
Assistant Inspector General for Information Technology Audits
U.S. Department of Transportation

Before the Committee on Transportation and Infrastructure
United States House of Representatives

Chairman DeFazio, Ranking Member Graves, and Distinguished Members of the Committee:

Thank you for inviting me to testify today on securing our Nation's infrastructure in an evolving cybersecurity landscape. As you know, the Department of Transportation (DOT) aims to ensure the United States has the safest, most efficient, and modern transportation system in the world. DOT relies on over 400 information technology (IT) systems to carry out this mission, including systems that manage air traffic, administer hundreds of billions of dollars, and maintain sensitive information about the transportation industry. DOT's cybersecurity program must protect these systems from malicious attacks and other compromises that may put public safety or taxpayer dollars at risk.

DOT has expressed a commitment to improving its cybersecurity. Nevertheless, recent cyberattacks remind us why the Department must be prepared at all times to manage cyber threats, which may originate in unfriendly nation-states, international criminal syndicates, and even within the United States. Due to the increasing threat of sophisticated cyberattacks, DOT must frequently update its digital infrastructure, as well as its methodology for monitoring networks, detecting potential risks, identifying malicious activity, and mitigating threats to sensitive information and information systems.

Our office has long identified cybersecurity as one of the Department's top management challenges—a challenge that will be compounded as DOT embarks on implementing new requirements under the President's recent Executive Order to improve the Nation's cybersecurity.[1] My testimony today is based on our recent and ongoing audit work and will focus on DOT's challenges in three areas: (1) developing a comprehensive Departmentwide cybersecurity strategy to address recurring weaknesses, (2) protecting IT infrastructure and sensitive information at DOT Operating Administrations (OA), and (3) coordinating with other agencies and industry partners on cybersecurity in the transportation sector.

Summary

While DOT has formalized and documented most of the policies and procedures for its cybersecurity program, the Department continues to face significant challenges in its implementation. These challenges are due to persistent deficiencies caused by the inconsistent enforcement of an enterprise-wide information security program, ineffective communication with the OAs, leadership gaps, and inadequate efforts to remediate the issues associated with

[1] Executive Order 14028: Improving the Nation's Cybersecurity (May 12, 2021).

66 of our prior-year audit recommendations. As a result, DOT faces the risk that its mission-critical systems could be compromised. While working to strengthen its cybersecurity posture across the Department, DOT must also address ongoing challenges in protecting the IT infrastructure that its OAs manage and monitor. These challenges include selecting and implementing more stringent security controls[2] for the Federal Aviation Administration's (FAA) high-impact systems that are critical for safely managing air traffic. We also recently reported that the Federal Transit Administration's (FTA) financial management systems have several security control deficiencies that could affect its ability to approve, process, and disburse billions of dollars of grant funds. Furthermore, our ongoing series of audits of the cybersecurity postures at multiple OAs has identified security weaknesses that could compromise millions of sensitive data records, including personally identifiable information (PII). These weaknesses are of particular concern given that OA networks are connected to DOT's overall IT infrastructure, exposing it to further risk. Finally, as one of the lead agencies[3] in protecting the critical infrastructure of the Nation's transportation sector, DOT must effectively partner with other Federal agencies and the private sector to improve cybersecurity, such as when securing cloud-based services. Such efforts are critically important because the incapacitation or destruction of transportation assets, systems, and networks would have a debilitating effect on the Nation.

Background

New guidance from the President has changed the manner in which executive agencies must identify and manage risk associated with information systems. Issued on May 12, 2021, Executive Order 14028: Improving the Nation's Cybersecurity, directs the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to persistent and increasingly sophisticated malicious cyber campaigns that threaten the public and private sectors and ultimately the security and privacy of the American people. To protect our Nation from malicious cyber actors and foster a more secure cyberspace, the Order also requires the Federal Government to partner with the private sector, which must adapt to the continuously changing threat environment and ensure its products are built and operate securely.

DOT's Office of the Chief Information Officer (OCIO), under authority granted by the Secretary of Transportation, has issued the *Departmental Cybersecurity*

[2] Security controls are safeguards or countermeasures designed to protect the confidentiality, integrity, and availability of information that is processed, stored, or transmitted by systems or organizations and to manage information security risk.

[3] The other lead agency is the Department of Homeland Security.

Policy,[4] which establishes the policies, processes, procedures, and standards of the DOT cybersecurity program. The policy also implements the mandatory requirements specified for all Federal agencies in the Federal Information Security Modernization Act of 2014 (FISMA), as amended,[5] and other laws, regulations, and standards related to information security, information assurance, and network security. FISMA requires Federal agencies to develop, document, and implement agencywide cybersecurity programs to protect the information and information systems that support their operations and assets. Under FISMA, DOT must provide information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of:

- information collected or maintained by or on behalf of DOT; and
- information systems used or operated by DOT employees or contractors or by another organization on DOT's behalf.

DOT is also required to implement mandatory cybersecurity requirements issued by other entities, including, but not limited to, the White House, Congress, Department of Homeland Security (DHS), Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST). The Department has adopted NIST's Risk Management Framework as the standard methodology for security authorization for its information systems and continuous monitoring of security controls.

Developing a Comprehensive Departmentwide Cybersecurity Strategy To Address Recurring Weaknesses

For the most part, DOT has formalized and documented its cybersecurity policies and procedures for protecting its information systems and data. Specifically the *Departmental Cybersecurity Policy*, and its supplement, the *Departmental Cybersecurity Compendium*, authorize DOT's Chief Information Officer (CIO) to secure all IT, information systems, networks, and data that support DOT operations. Moreover, in the wake of increased telework during the Coronavirus Disease 2019 (COVID-19) pandemic, the OCIO upgraded security and tripled departmental network bandwidth. These actions ensured that employees working from home could access systems and data to fulfill their responsibilities.

[4] DOT Order 1351.37, *Departmental Cybersecurity Policy*, July 14, 2017.

[5] Pub. L. No. 113-283 (December 18, 2014).

The Department's formal policies align with Federal guidelines—specifically, those for security controls for identifying and managing risks, protecting information systems, detecting potential cybersecurity incidents, and responding to and recovering from incidents. However, DOT does not implement them in a consistent or comprehensive manner. As a result, the Department faces the risk that its mission-critical systems could be compromised.

Since 2003, we have conducted annual reviews of DOT's information security programs and practices, in accordance with FISMA requirements. As we reported in our most recent FISMA audit,[6] the Department has yet to address longstanding cybersecurity deficiencies related to its practices for protecting its mission-critical systems from unauthorized access, alteration, or destruction. For example, we continue to note inconsistencies in DOT's implementation of its cybersecurity program (see table).

Table. Weaknesses in DOT's Implementation of Its Cybersecurity Program

Category	Issues OIG Identified in 2021
Risk management	*Inventories:* DOT did not maintain accurate and complete inventories of all OA information systems and was unable to demonstrate that it had a formal process in place for ensuring the accuracy and completeness of the hardware asset inventories it reports to OMB—key prerequisites to an effective risk-management program.
	Security controls: DOT did not always test the security controls for its information systems or properly approve security assessment and authorization documentation.
	Tracking vulnerabilities: DOT did not always report, manage, and close security weaknesses identified in plans of action and milestones (POA&M).
	Supply chain risk management: DOT has not developed a supply chain risk management strategy and implementation plan to ensure that external providers comply with departmental cybersecurity requirements.
Protecting DOT's information systems from risk of compromise	*Configuration management:* DOT has not consistently remediated vulnerabilities related to unsupported operating systems, unpatched applications, and configuration weaknesses, which may allow unauthorized access into mission-critical systems and data.
	Identity and access management: Employees and contractors do not always access the DOT network with personal identity verification (PIV) cards because many Department systems are not enabled to use PIV cards or do not require them.
	Data protection and privacy: DOT does not always review privacy documentation designed for the protection of PII each year; in some cases, the documentation is not current or has not been developed. This puts the PII stored in DOT's information systems at risk for compromise.

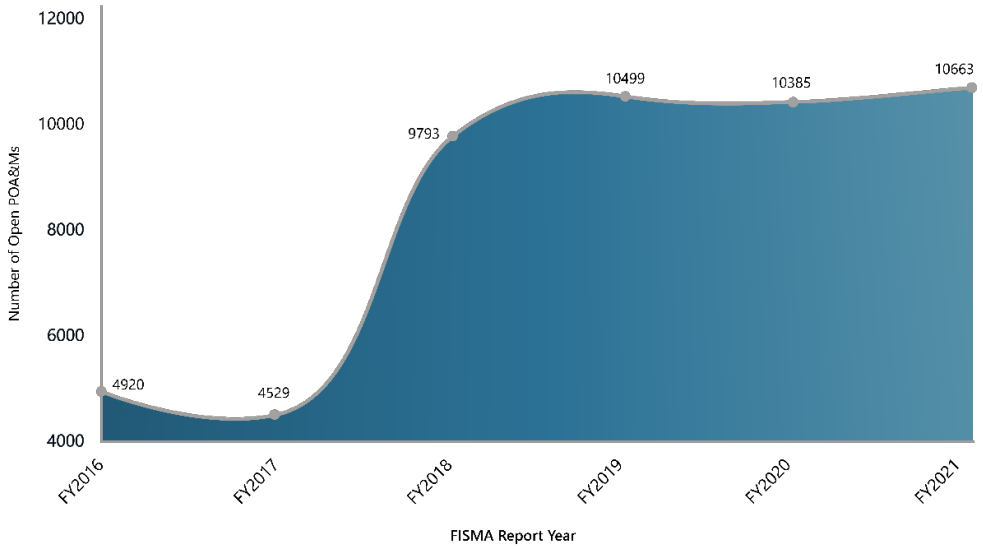
[6] *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security System Program and Practices* (OIG Report No. QC2022006), October 25, 2021. OIG reports are available on our website: https://www.oig.dot.gov/.

Category	Issues OIG Identified in 2021
Detecting potential cybersecurity threats	*Information security continuous monitoring:* DOT does not conduct annual security control assessments on some systems. As a result, it lacks an ongoing awareness of information security, vulnerabilities, and threats to systems and information.
Responding to cybersecurity incidents	*Incident response:* DOT did not provide evidence that it evaluates the effectiveness of its incident response technologies or adjusts configurations and toolsets as appropriate, raising questions about the effectiveness of its automated detection capabilities. DOT's Security Operations Center also does not have file-integrity checking software for detecting signs of cyber incidents.
Recovering from cybersecurity incidents	*Contingency plans:* DOT does not test all of its contingency plans on an annual basis; other plans have not been developed, reviewed, or updated in a timely manner. Comprehensive testing is crucial to ensure organizational systems and data are available and that IT systems and applications can function during outages.

Source: Independent auditor analysis

Many of these and other weaknesses can be attributed to the Department's lack of progress in addressing our 66 prior-year audit recommendations. DOT has struggled to remediate its security weaknesses in a timely manner and has yet to close 10,663 vulnerabilities associated with its information systems, as compared with the 10,385 weaknesses we found in 2020.[7] Figure 1 identifies the number of DOT plans of action and milestones (POA&M) that have remained open for the past 6 years.

Figure 1. Total Number of Open Departmentwide POA&Ms Since FY 2016



Source: OIG analysis of DOT data

[7] *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security Program and Practices* (OIG Report No. QC2021003), October 26, 2020.

Furthermore, as early as 2012, we identified high-risk security vulnerabilities—including inconsistent software updates—that an attacker could exploit to control systems or access files and data. Since 2013, DOT has not had a comprehensive and accurate inventory of its information systems and, as a result, may be unable to identify and address all system vulnerabilities. The Department has also not resolved our 2018 recommendation to develop and maintain accurate inventories of cloud systems, contractor systems, and websites that allow public access. The lack of accurate inventories of its hardware assets may be even more critical in light of the increased use of telework in response to COVID-19.

These vulnerabilities are compounded by the inconsistent enforcement of a Departmentwide information security program. For one, DOT has not had a permanent Chief Information Security Officer with the leadership authority to perform effective oversight and ensure accountability for departmental information security improvements for close to a year. Thus, it is challenging for DOT to move forward with a continuity of strategy that can affect long-term changes. To address these longstanding and recurring cybersecurity weaknesses, we made one overarching key recommendation to the Department this year: require the OCIO to develop a multiyear strategy and approach—complete with objective milestones and resource commitments—to implement the necessary corrective actions to ensure an effective information security program. To DOT's credit, it agreed with our recommendation and directed the CIO to develop and implement such an approach by December 2022.

Protecting IT Infrastructure and Sensitive Information at DOT Operating Administrations

Our recent audit work shows that DOT faces ongoing challenges protecting the IT infrastructure that its OAs manage and monitor. This infrastructure includes systems that are integral to the safe and efficient operation of our Nation's transportation system; help manage the disbursement of billions of dollars to grantees; and contain sensitive information, including PII.

Strengthening Security Controls for High-Impact Systems at FAA

The Department faces some of its most significant cybersecurity challenges at FAA, which owns 325—or about 75 percent—of DOT's 431 information technology systems. Specifically, FAA operates a vast network of systems and facilities for managing air traffic in the National Airspace System (NAS). This

complex network has evolved over the years into an amalgam of diverse legacy radars and newer satellite-based systems for tracking aircraft, as well as a new initiative for controllers and pilots to share information through data link communications.

Recognizing the importance of protecting its infrastructure from rapidly evolving cyber-based threats, FAA recently re-categorized 45 low- and moderate-impact systems as high impact. According to the Federal Information Processing Standards,[8] a high-impact system is one in which a security breach or loss is expected to have a severe or catastrophically adverse effect on organizational operations, assets, or individuals. For example, one of the recently re-categorized systems is the En Route Automation Modernization system, which air traffic controllers rely on to manage high-altitude air traffic nationwide.

Re-categorizing a system as high impact creates more stringent security control requirements to safeguard the confidentiality, integrity, and availability of information processed or stored on the system. However, we recently reported that FAA lacks formalized policies and procedures for selecting and implementing high security controls for its high-impact systems.[9] As FAA's reliance on interconnectivity increases, so does the risk of cybersecurity breaches, which can have a significant impact on the NAS. To increase cybersecurity, FAA must complete its selection and implementation of all required high-security controls for these mission-critical systems.

Protecting FTA's Financial Management Systems

We recently reported[10] that FTA's financial management systems have several security control deficiencies that could affect the Agency's ability to approve, process, and disburse grant funds, including nearly $70 billion in COVID-19 relief appropriations. Security controls for FTA financial management systems are especially critical given that the transit industry is vulnerable to cyberattacks. For example, we reported that in 2020 and 2021, at least five FTA grant recipients were victims of cyberattacks that exposed PII, personnel data, and financial data. Grant recipients' security incidents may result in the compromise of usernames

[8] Federal Information Processing Standards Publication 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[9] *FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented* (OIG Report No. IT2021033), August 2, 2021.

[10] *FTA Does Not Effectively Assess Security Controls or Remediate Cybersecurity Weaknesses To Ensure the Proper Safeguards Are in Place To Protect Its Financial Management Systems* (OIG Report No. IT2022005), October 20, 2021.

and credentials and expose FTA to cyberattacks that may delay the distribution of COVID-19 related funds to recipients.

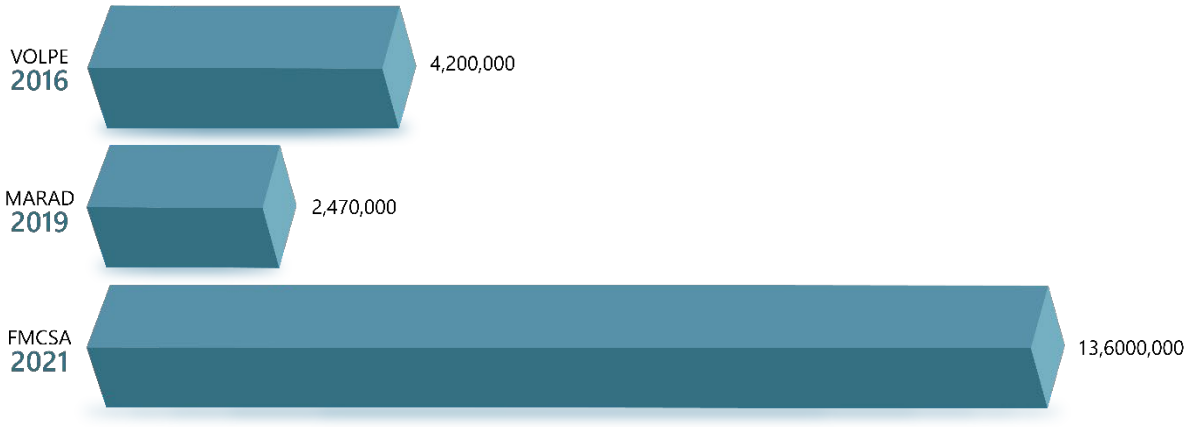
Despite these risks, we found that FTA did not always effectively select, document, implement, and monitor the security controls for its financial management systems. For example, FTA security officials reported that 139 of 269 security controls were satisfied, but we found they were not tested or implemented as required. As a result of these and other issues, FTA officials may not have accurate pictures of security risks. Additionally, FTA has not remediated longstanding security control weaknesses that it has identified since 2016—including issues with multifactor authentication—which increases the risk that malicious actors could gain unauthorized access. Other weaknesses include unsecure databases, a lack of integrity monitoring tools, and insufficient contingency and incident response planning. If compromised, these weaknesses could lead to a cybersecurity attack.

Safeguarding PII by Preventing Cyberattacks at Multiple OAs

Several of our recent reviews have raised concerns regarding whether the OAs have the appropriate security controls in place to protect DOT's networks and information systems from unauthorized access, including insider threats. In our recent audits of the cybersecurity postures at the Volpe National Transportation Systems Center (Volpe), Maritime Administration (MARAD), and Federal Motor Carrier Safety Administration (FMCSA),[11] we identified and could have exploited security weaknesses and accessed millions of data records. As part of our vulnerability assessments and penetration testing, we were able to access to millions of sensitive records, including PII (see figure 2).

[11] *The Volpe Center's Information Technology Infrastructure Is at Risk for Compromise* (OIG Report No. FI2016056), March 22, 2016; *The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise* (OIG Report No. FI2019057), July 24, 2019; *FMCSA's IT Infrastructure Is at Risk of Compromise* (OIG Report No. IT2022003), October 20, 2021.

Figure 2. Number of Unauthorized PII Records That OIG Was Able To Access at Volpe, MARAD, and FMCSA



Source: Results of OIG audits of Volpe, MARAD, and FMCSA security postures conducted in 2016, 2019, and 2021, respectively.

For example, we successfully penetrated FMCSA's infrastructure and gained unauthorized access to 13 million PII records. If breached, these systems could have cost the Department millions of dollars in credit monitoring fees to protect affected individuals from identity theft. We also identified recurring weaknesses that we could exploit, including poor security practices, such as weak administrative-level login credentials, unpatched servers and workstations, and a lack of encryption of sensitive data.

Many of the weaknesses we found at FMCSA also tie into the same persistent enterprise-level security risks we found during our audits of MARAD and Volpe's IT networks and systems. These weaknesses are of particular concern given that these OAs' networks process, store, and transmit a substantial amount of sensitive information and are connected to DOT's overall network. Until the Department implements appropriate safeguards and countermeasures to protect its networks, DOT and its OAs will continue to be at risk for an enterprise-wide cybersecurity attack that could have a major impact on mission-critical systems. We plan to continue to review the IT infrastructure at individual OAs; our fourth audit in this series will focus on the Federal Highway Administration.

Coordinating With Other Agencies and Industry Partners To Ensure Cybersecurity in the Transportation Sector

As a lead agency in protecting the critical infrastructure of the Nation's transportation sector, DOT must partner effectively with other Federal agencies and industry to mitigate vulnerabilities and ensure cybersecurity. Both DHS and DOT have the authority and responsibility to protect the U.S. transportation sector from physical and cyber threats.[12] DOT also coordinates with other Federal agencies and industry partners. For example, the FAA Extension, Safety, and Security Act of 2016 directs FAA to develop a comprehensive, strategic framework to reduce cybersecurity risks to civil aviation. FAA's efforts to implement this framework involve coordinating and collaborating on aviation cybersecurity with DHS and the Department of Defense through the Aviation Cyber Initiative. Protecting flight-critical systems—and the safety of the flying public—from rapidly evolving cyber-based threats also requires the cooperation of aviation stakeholders from industry, airlines, airports, and manufacturers.

DOT's collaboration and coordination across the transportation sector is of critical importance because the incapacitation or destruction of transportation assets, systems, or networks would have a debilitating effect on the Nation's security, economy, and public health and safety. On May 8, 2021, for example, the Colonial Pipeline Company announced that it had halted its pipeline operations due to a ransomware attack, disrupting critical supplies of gasoline and other refined products throughout the East Coast. This incident and other cyberattacks have elevated concerns about the security of the Nation's critical infrastructure, including energy pipelines and the transportation sector.

Accordingly, we will monitor DOT's ongoing efforts to ensure cybersecurity in the transportation sector, particularly as it increasingly relies on private-sector partners for internet-based computing services (commonly referred to as cloud services) to address IT needs. To that end, we have initiated a review of the Department's strategy to secure cloud services and transition toward zero trust architecture, key provisions of Executive Order 14028. As defined by NIST,[13] zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), rather than network location, which is no longer seen as the prime

[12] See Executive Order 14028: Improving the Nation's Cybersecurity (May 12, 2021) and Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (February 12, 2013).

[13] NIST Special Publication 800-207, *Zero Trust Architecture*, August 2020. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or on asset ownership (enterprise or personally owned).

component of an entity's security posture. We will keep the committee updated on our progress in monitoring and assessing the Department's cybersecurity program, including its partnerships with the private sector and other agencies.

Conclusion

DOT's cybersecurity program is critical to protect its vast network of IT systems from malicious attacks and other breaches that pose a threat to the U.S. transportation system. In today's rapidly evolving cybersecurity landscape, and as the Nation embarks on a new journey to upgrade and improve its transportation infrastructure, DOT faces significant challenges in strengthening its systems while adapting to new and rising challenges and threats. We remain committed to supporting the Department's efforts as it works to remediate existing vulnerabilities and bolster DOT's overall cybersecurity posture. We will continue to update you on our work on these and related matters.

This concludes my prepared statement. I would be happy to address any questions from you or Members of the Committee at this time.

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety Hotline

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

OUR MISSION

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

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