Redacted Final Report
No. IT2023043
August 30, 2023

OST

DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture

~~Final Report Contains Information Marked~~

U.S. Department of Transportation
Office of Inspector General

Highlights

DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture

Self-Initiated

Office of the Secretary of Transportation | IT2023043 | August 30, 2023

What We Looked At

Over the past 10 years, the Department of Transportation (DOT) and its Operating Administrations (OA) have increased their migration to and adoption of cloud computing based on Federal requirements. In May 2021, the President issued Executive Order 14028 to modernize Federal Government cybersecurity by accelerating the movement to secure cloud services, adopting security best practices, and advancing towards zero trust architecture (ZTA). Given the administration's increased emphasis on cloud services, we initiated this audit. Our audit objectives were to assess the effectiveness of the Department's (1) cloud systems' security and privacy controls and (2) strategy to secure cloud services in order to implement ZTA.

What We Found

DOT and its OAs do not consistently implement security and privacy controls to protect their cloud-based systems. First, the Department and several OAs did not effectively follow Federal requirements and best practices to protect their cloud systems from cyberattacks. Second, DOT does not always effectively manage and secure the computing resources for its cloud-based systems by using secure configuration baselines, implementing multifactor authentications, encrypting data, or updating software. Lastly, DOT does not consistently use the appropriate mechanisms to detect, mitigate, and report cyberattacks on the Department's and most of the OAs' cloud-based systems. As a result, DOT may not have visibility into cybersecurity incidents, exposing it to potential threats and security weaknesses. Furthermore, DOT lacks an effective strategy for securing its cloud services transition to ZTA because its current ZTA implementation plan does not include a proposed schedule or migration steps as required by Federal guidelines. This may cause DOT to miss key milestones for implementing ZTA by the end of fiscal year 2024. Therefore, the Department will not be well positioned to meet ZTA's intent to maximize security and minimize uncertainty of computing systems.

Our Recommendations

We made 21 recommendations to improve the Agency's cloud services program and transition its enterprise network to ZTA. DOT concurred with 19 of 21 recommendations, did not concur with 1 recommendation, and asked to close 1 recommendation. We consider 17 of 19 recommendations resolved but open pending completion of planned corrective actions and request DOT provide an updated response for the 2 other recommendations. We consider two recommendations unresolved and request the Agency reconsider its non-concurrence for the first recommendation and provide documentation to support closing the second recommendation.

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

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

Contents

U. S. Department of Transportation
Office of Inspector General

Memorandum

Date: August 30, 2023

Subject: ACTION: DOT's Cloud-Based Systems' Security Weaknesses Hinder Its Transition to a Zero Trust Architecture | Report No. IT2023043

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

Dorsey

To: Chief Information Officer

Issued in 2011, the Federal Cloud Computing Strategy[1] encouraged Government agencies to increase the use of cloud computing[2] services. Specifically, this policy encouraged agencies to modify their Information Technology (IT) portfolios to take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. In 2019, the Office of Management and Budget (OMB) updated the strategy, tasking agencies with accelerating their migration to cloud-based solutions to modernize IT infrastructure, enhance security, and provide high-quality IT services for the American people.

Over the past 10 years, the Department of Transportation (DOT) and its Operating Administrations[3] (OA) have increased their migration to and adoption of cloud computing based on Federal requirements. Currently, the Department has 29 Federal Information Security Modernization Act (FISMA)–reportable[4] cloud systems. OA security officials (i.e., system owners and information system security managers) are responsible for managing their information system inventories. The Department defines the policies and procedures OAs must follow when a system is categorized as a cloud computing resource. However, based on our past work, the Department lacks a comprehensive and accurate inventory of its

[1] Office of Management and Budget (OMB), *Federal Cloud Computing Strategy*, February 8, 2011.
[2] Cloud computing relies on internet-based interconnectivity and resources to provide computing services to customers, while intending to free customers from the burden and costs of maintaining the underlying infrastructure.
[3] The Department's Operating Administrations include 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, and Pipeline and Hazardous Materials Safety Administration, as defined in 49 C.F.R. § 1.2.
[4] DOT *FISMA Inventory Guide*, version 1.1, September 2013.

cloud systems[5]—a key requirement for effective information system risk management. Moreover, most Federal agencies that use cloud services, including DOT, contract out these services to third-party companies. For example, DOT and its OAs—such as the Federal Aviation Administration (FAA), Federal Highway Administration (FHWA), Federal Railroad Administration (FRA), and Maritime Administration (MARAD)—currently use at least two major cloud service providers[6] (CSP). However, we previously found the Department does not always follow Federal requirements when performing security assessments of its cloud systems and does not properly authorize the use of CSP services,[7] and we continue to have an open recommendation regarding these security risks.

In May 2021, the President issued Executive Order (EO) 14028,[8] detailing the administration's goal to modernize Federal Government cybersecurity by accelerating the movement to secure cloud services, adopting security best practices, and advancing toward zero trust architecture (ZTA). Specifically, zero trust provides a collection of concepts and ideas designed to maximize security and minimize uncertainty for computing systems. The foundational tenet of the zero trust model is that no actor, system, network, or service is trusted, regardless of whether it is operating outside or within the security perimeter. Instead, agencies must verify anything and everything that attempts to establish access.

Given the administration's increased emphasis on cloud services, we initiated this audit to assess DOT's oversight of its cloud services and the overall effectiveness of its cloud systems' security and privacy controls. Accordingly, our audit objectives were to assess the effectiveness of the Department's (1) cloud systems' security and privacy controls and (2) strategy to secure cloud services in order to implement ZTA.

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the organizations we visited or contacted, and exhibit C lists the acronyms used in this report.

[5] *Quality Control Review of the Independent Auditor's Report on the Assessment of DOT's Information Security System Program and Practices* (OIG Report No. QC2022042), September 28, 2022. OIG reports are available on our website: https://www.oig.dot.gov/.

[6] Cloud service providers develop infrastructure, platforms, and software application services that can be shared by multiple customers. Each customer can buy the number of services needed and make adjustments as needed.

[7] *DOT Lacks An Effective Process For Its Transition to Cloud Computing* (OIG Report No. FI2015047), June 6, 2015.

[8] Exec. Order 14028, *Improving the Nation's Cybersecurity*, May 2021.

We appreciate the courtesies and cooperation of DOT representatives during this audit. If you have any questions concerning this report, please contact me or Stacy Jordan, Program Director.

cc: The Secretary
DOT Audit Liaison, M-1

Results in Brief

DOT and its OAs do not consistently implement security and privacy controls to protect their cloud-based systems.

First, the Department and several of its OAs do not effectively follow Federal requirements and best practices to protect their cloud systems from cyberattack, such as by continuously monitoring cloud services for security weaknesses. Second, DOT does not always effectively manage and secure the cloud computing resources for its cloud-based systems. For example, DOT's cloud-based systems do not continually use secure configuration baselines to protect servers, network devices, and data; implement multifactor authentication (MFA) to prevent unauthorized access to its systems; encrypt data to protect private and sensitive information; and keep software up to date to protect applications and data. Lastly, DOT does not consistently use the appropriate mechanisms to detect, mitigate, and report cyberattacks on its cloud-based systems. Specifically, DOT does not regularly monitor the Department's and most of the OAs' cloud-based systems for potential cybersecurity incidents. The exception is FAA, for which DOT's security operations center (SOC) has the necessary visibility into FAA's cloud-based systems. As a result, DOT may not have the necessary visibility into its cloud-based systems cybersecurity incidents, and more importantly, the lack of SOC monitoring could expose the Department to potential threats and security weaknesses.

DOT lacks an effective strategy for securing its cloud services transition to ZTA.

In January 2022, OMB Memorandum M-22-09[9] established a Federal ZTA strategy. As part of this strategy, agencies are required to meet specific cybersecurity standards and objectives by the end of fiscal year 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threats. According to a DOT Office of the Chief Information Officer (OCIO) official, the Department is currently developing its strategy for securing cloud services in order to implement ZTA by OMB's deadline. In accordance with EO 14028 and M-22-09, the Department was required to provide OMB with its ZTA implementation plan, complete progress reports on implementing MFA,[10] encrypt data at rest[11]

[9] OMB, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles* (M-22-09), January 26, 2022.

[10] Multifactor authentication requires using two or more different factors to achieve authentication. The factors are frequently described as including "something you know" (e.g., PIN, password) and "something you have" (e.g., personal identity verification [PIV] cards, token).

[11] Encryption of data at rest protects stored data from a system compromise or data exfiltration.

and in transit[12] until ZTA is fully adopted Departmentwide; and designate a ZTA implementation lead. However, the Department's ZTA implementation plan does not include a proposed schedule or the migration steps necessary for the successful transition to ZTA. This lack of strategy for a secure cloud services transition to zero trust may cause DOT to miss key administration milestones for achieving ZTA implementation by the end of fiscal year 2024. Therefore, the Department will not be well positioned to meet the intent of ZTA, which is to maximize security and minimize uncertainty with computing systems.

Background

Cloud computing is a model for enabling on-demand remote access to a shared pool of configurable computing resources (i.e., networks, virtual servers,[13] applications,[14] and services). These resources can be rapidly provisioned and released from CSPs with minimal management effort or human interaction. Cloud computing relies heavily on automated technologies and virtualization—the simulation of the software and/or hardware upon which other software runs.

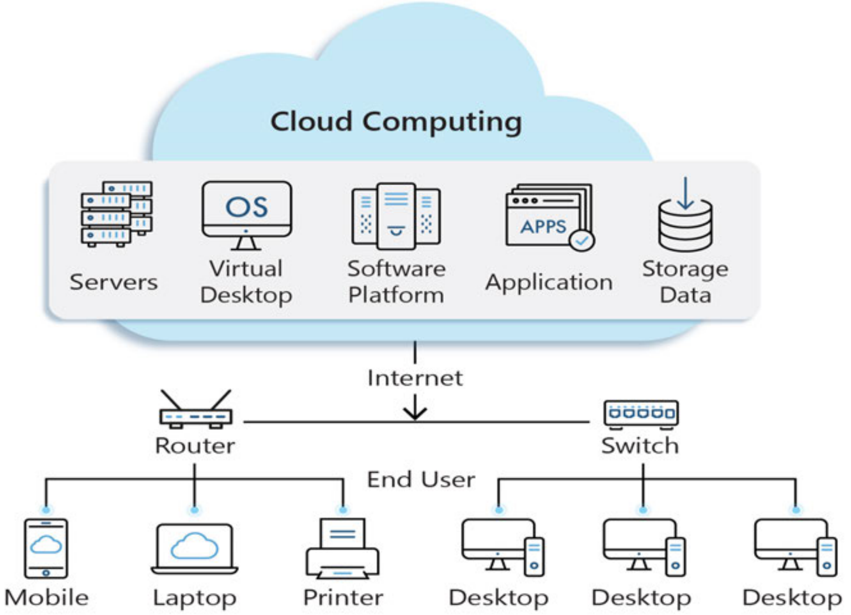
Figure 1 presents a graphical representation of the cloud computing environment, depicting a virtual desktop operating system (OS) that runs all the hardware, software, applications, and data and operates on a virtual central server. It is separated from what end users see on their physical devices (e.g., mobile, laptop, and desktop), which use communication protocols through routers and switches to remotely access the cloud computing environment over the internet.

[12] Encryption of data in transit offers protection in case communications are intercepted while data moves between your site and the cloud provider or between two services.

[13] Cloud servers are virtual (not physical) servers running in a cloud computing environment that can be accessed on demand by unlimited users. Cloud servers work just like physical servers, and they perform similar functions like storing data and running applications.

[14] An application is a computer software program that performs a specific function directly for an end user and, in some cases, for another application.

Figure 1. Cloud Computing Relationship to End User



Source: OIG-refined depiction of cloud computing

OMB established the Federal Risk and Authorization Management Program (FedRAMP) in 2011 to provide a standardized, cost-effective, risk-based approach for the Government's adoption and use of cloud services. FedRAMP allows agencies to select and authorize the use of cloud services in accordance with FISMA and the National Institute of Standards and Technology's (NIST) security requirements. It also empowers agencies to use modern cloud technologies, with an emphasis on securing and protecting Federal information. OMB required all executive branch agencies to use FedRAMP for authorizing all cloud services by June 2014.[15]

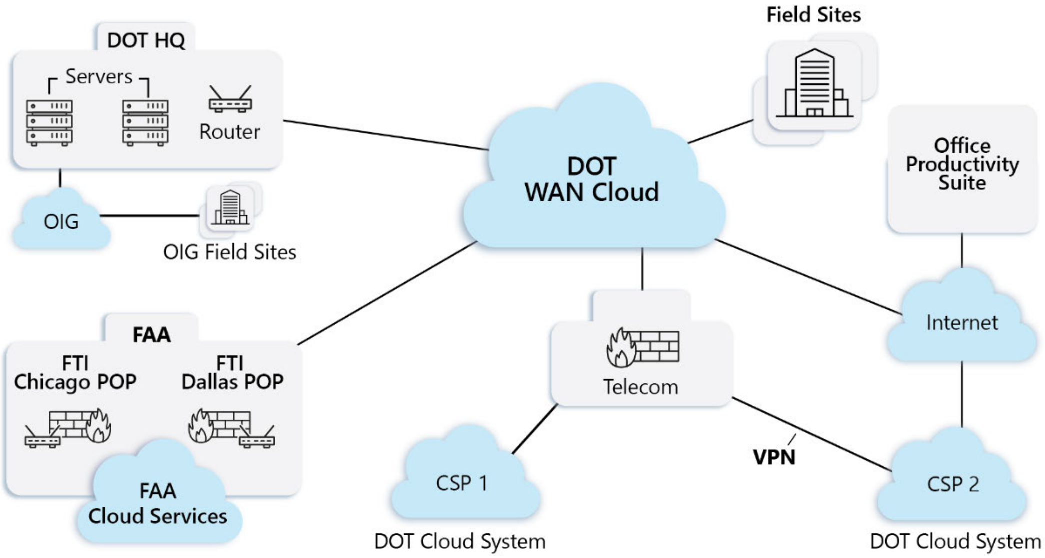
The partnership between CSPs and agencies in designing, building, deploying, and operating cloud-based systems presents new challenges for providing end users with adequate security and privacy protection. CSPs and agencies must collaborate and share the responsibility for implementing the necessary controls.

DOT currently uses a variety of cloud service offerings (CSO) and deployment models to provide internal and external stakeholders with core email services, messaging and collaboration programs, office productivity tools, select application workloads, and cloud storage for user data. These are provided to DOT and its OAs by at least two major CSPs, which have several CSOs. Figure 2

[15] OMB, *Security Authorizations of Information Systems in Cloud Computing Environment*, December 8, 2011.

depicts DOT's wide area network (WAN)[16] cloud design for its enterprise, including FAA and the Office of Inspector General (OIG), which primarily provision their own cloud services.

Figure 2. DOT's Cloud Network Design



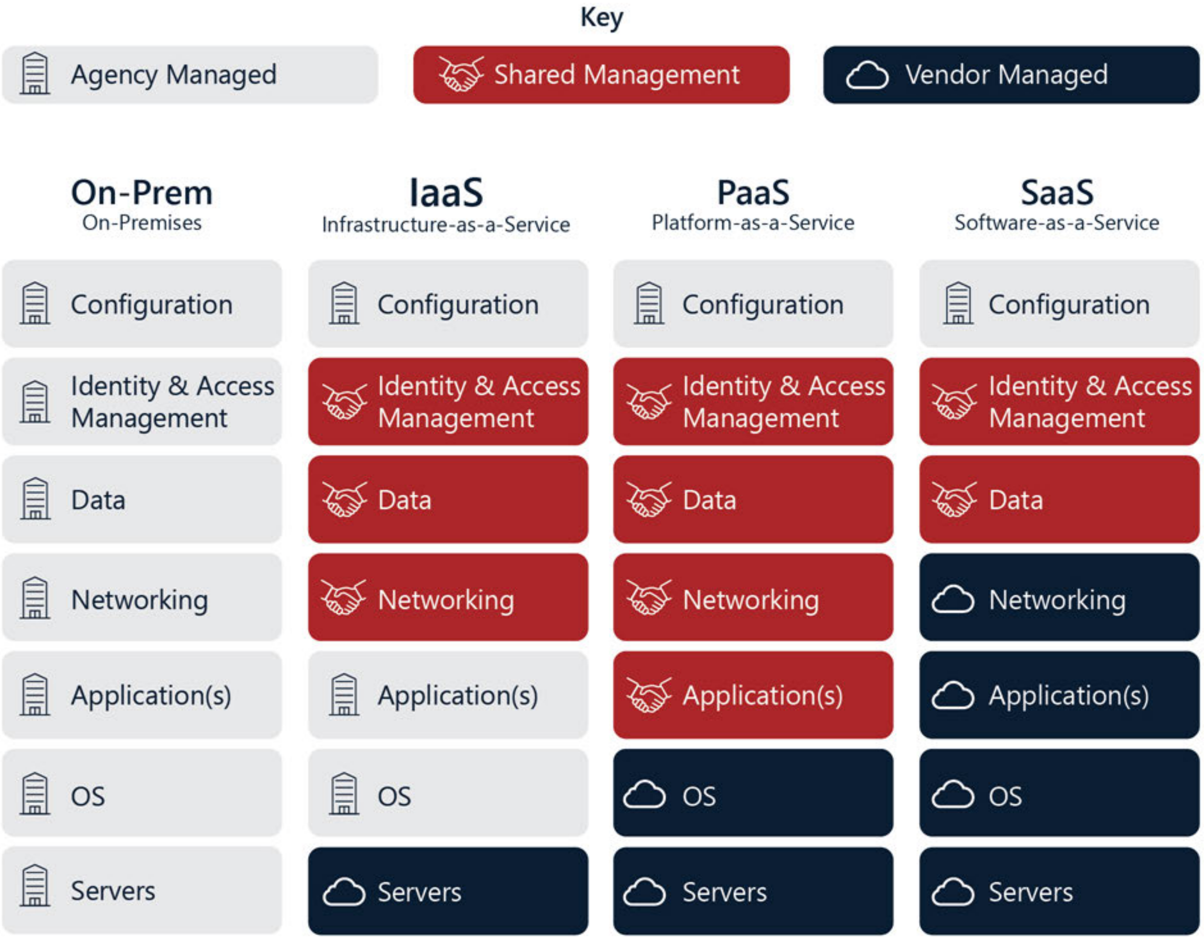
Source: OIG-refined depiction of DOT's cloud network design, June 2022

The Cybersecurity and Infrastructure Security Agency (CISA), in consultation with the U.S. Digital Service and FedRAMP, developed the Cloud Security Technical Reference Architecture[17] to illustrate recommended approaches to cloud migration and data protection. While there are many options for moving an agency's on-premise applications, services, or infrastructure (e.g., networks and servers) into the cloud, NIST has defined three basic cloud service models—Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS)—as the most prevalent. CISA's shared security model shows how each service model is consumed and protected (see figure 3). The model depicts whether the agency, CSP, or both parties hold responsibility for managing SaaS, IaaS, and PaaS, and the associated information systems' computing resources in the cloud environment. The model also highlights various layers within cloud systems that require protection and management, including systems configuration, identity and access management, data, networking, applications, OS, and servers.

[16] A wide area network is a geographically distributed private telecommunications network that interconnects multiple local area networks.

[17] Cybersecurity and Infrastructure Security Agency (CISA), *Cloud Security Technical Reference Architecture*, August 2021.

Figure 3. Shared Security Model—Agency, Shared, and Vendor-Managed Responsibilities for Each Cloud Service Model



Key

⬜ Agency Managed 🟥 Shared Management ⬛ Vendor Managed

On-Prem On-Premises	IaaS Infrastructure-as-a-Service	PaaS Platform-as-a-Service	SaaS Software-as-a-Service
⬜ Configuration	⬜ Configuration	⬜ Configuration	⬜ Configuration
⬜ Identity & Access Management	🟥 Identity & Access Management	🟥 Identity & Access Management	🟥 Identity & Access Management
⬜ Data	🟥 Data	🟥 Data	🟥 Data
⬜ Networking	🟥 Networking	🟥 Networking	⬛ Networking
⬜ Application(s)	⬜ Application(s)	🟥 Application(s)	⬛ Application(s)
⬜ OS	⬜ OS	⬛ OS	⬛ OS
⬜ Servers	⬛ Servers	⬛ Servers	⬛ Servers

Source: OIG-refined depiction of the security service model in CISA's Cloud Security Technical Reference Architecture, August 2021

The three cloud services models provide the following services:

- **SaaS:** The agency uses the CSP application(s) running on its cloud infrastructure and available through various client platforms (e.g., web-based emails). The CSP is responsible for managing and securing the underlying cloud infrastructure including network, servers, OS, and even individual application capabilities.

- **IaaS:** The agency has the capability to provision processing, networks, and other fundamental computing resources, as well as to deploy and run arbitrary software, which can include applications and OS, on the cloud infrastructure. The CSP is responsible for managing or controlling the underlying cloud infrastructure (e.g., servers), while the agency is responsible for software updates and controlling the provisioned OS and deployed applications software.

- **PaaS:** Similar to an IaaS, the PaaS allows the agency to deploy custom applications using the CSP's supplied programming languages, services, and tools on the cloud infrastructure. The CSP is responsible for managing or controlling the underlying cloud infrastructure including network, servers, and OS, but agencies share responsibility for managing and securing the deployed applications.

There are four ways cloud service models can be deployed in the cloud:[18]

1. Private: The cloud infrastructure is provisioned for exclusive use of an organization comprised of multiple customers (e.g., an agency with multiple business units).

2. Community: The cloud infrastructure is provisioned to a specific community of consumers that have shared concerns (e.g., mission-security requirements, policy, and compliance considerations).

3. Public: The cloud infrastructure is provisioned for use by the general public.

4. Hybrid: The cloud infrastructure is composed of two or more of the above-mentioned cloud service models.

NIST provides a catalog of security and privacy controls for Federal information systems and organizations and a process to select controls to protect organizational assets from a set of threats, including cyberattacks and human error.[19] Information system services provided by external providers for conducting important mission and business functions, such as cloud-based services, must meet the same security requirements as Federal agencies. Specifically, CSPs are required to comply with FedRAMP security authorization requirements, such as assessing security controls for external information systems and performing continuous monitoring activities.

Agencies like DOT use contracts or service level agreements (SLA) to communicate requirements to their selected CSP(s). Therefore, agencies should carefully set up SLAs to define and set agency expectations and CSP-specific responsibilities. However, agencies are ultimately responsible for securing and protecting their information and services in the cloud.

[18] CISA, *Cloud Security Technical Reference Architecture*, August 2021.

[19] NIST Special Publication 800-53 rev. 4, *Security and Privacy Controls for Federal Information Systems*, April 2013.

According to OMB's Cloud Smart Strategy,[20] agencies should take a risk-based approach to securing the cloud within their network environment. Given the distributed nature of cloud services and the growing number of discrete capabilities and available deployment models, an agency may apply or incorporate protecting security and privacy controls to the data layer itself instead of at the network perimeter.

DOT and Its Operating Administrations Did Not Consistently Implement Security and Privacy Controls for Protecting Cloud-Based Systems

The Department and most of its OAs did not fully adhere to Federal requirements and best practices for cloud systems. This is critical because DOT's cloud-based systems have security weaknesses that could put data and networks at risk of compromise. Moreover, DOT did not consistently use the appropriate mechanisms to detect, mitigate, and report cyberattacks.

DOT and Several OAs Did Not Regularly Follow Federal Requirements and Best Practices for Cloud Systems

Security officials in DOT's OCIO have not developed specific policies and procedures for DOT's and its OAs' adoption and use of cloud services. The exception is FAA, which has implemented its own policies and procedures. OMB requires agencies to define, implement, and maintain processes, standards, and policies for all information resources—in support of their missions and business needs and in coordination with program managers.[21] According to OCIO officials, developing cloud-based policy and procedures has been an evolutionary process, and their overall strategy for the cloud services program is in a draft phase and was scheduled to be completed by the end of 2022, but the OCIO has yet to do so. The lack of specific cloud services policy and procedures leaves DOT without a governance process to enforce its OAs' adherence to Federal guidelines for cloud services. Additionally, it leaves the Department without a clear cloud computing strategy that allows it to fully take advantage of cloud computing benefits and

[20] OMB, *Federal Cloud Computing Strategy*, June 2019.
[21] OMB, Circular A-130, *Managing Information as a Strategic Resource*, July 2016.

thus maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost.

Specifically, DOT does not consistently follow FEDRAMP as required by law to protect Federal data stored in the cloud or properly authorize cloud services in a way that demonstrates its understanding of FedRAMP requirements. Federal agencies like DOT are required to use FedRAMP when conducting risk assessments, security authorizations, and granting Authorization to Operate (ATO) letters for the use of cloud services. However, we found that:

- DOT only had three of nine OAs submit an ATO letter to the FedRAMP Program Management Office (PMO) before they adopted and used cloud services unless they were leveraging an existing ATO letter. As a result, only FAA, FHWA, and the Federal Transit Administration (FTA)—the three OAs that submitted ATO letters for their cloud services—have assurance that their cloud services adhere to FedRAMP security baselines.

- FedRAMP's PMO also uses agency ATO letters to determine which Federal departments and agencies use a particular cloud service offering and/or provider. However, because DOT does not consistently provide the required ATO documentation to the FedRAMP PMO, we could not verify whether the Department was maintaining an accurate inventory of cloud services or CSPs.

- DOT and its OAs—with the exception of FAA, FHWA, and FTA—do not conduct quality and risk assessments of their CSP authorization package for CSOs. Such reviews ensure that the authorization package clearly and accurately reflects the security posture of the CSO and allow DOT's Authorizing Official to make an informed and risk-based authorization decision as required by FedRAMP.

In addition, DOT reported that it uses standard cloud clauses in contracts for CSP services to ensure they are secure. However, we found that two contracts for DOT's enterprise cloud services as well as other cloud services contracts for FAA, MARAD, and the Office of the Secretary (OST) did not have the required security clause language. DOT's acquisition policy states that contracting officers shall insert the required standard cloud clause into all solicitations and contracts, including task orders if appropriate, for information systems in the cloud computing environment.[22] However, departmental and OA procurement officials do not regularly insert the required security requirements into cloud services contracts. Specifically, four of nine DOT OAs and components' cloud contracts

[22] DOT Acquisition Policy, DASH-2016-03, *Federal Information Technology Systems Security Requirement for Unclassified Cloud Contract Language*, 2016.

contained the required security requirements. Consequently, DOT and OA security officials cannot ensure the awarded contractor will perform the necessary security activities, such as security control assessments, for cloud-based information systems.

Furthermore, DOT components and OAs have not always used SLAs as required for establishing and maintaining trust with their CSPs. We found that six of eight OAs and one DOT component—FAA, FMCSA, FRA, the National Highway Safety Administration (NHTSA), MARAD, Pipeline and Hazardous Materials Safety Administration (PHMSA), and OST—did not have SLAs in place. Specifically, departmental and OA procurement officials did not establish SLAs between the DOT component and the relevant CSPs. Without an SLA that covers DOT cloud services, the contract lacks appropriate measures to address specific details on the types of services, responsibilities, expected performance levels (e.g., acceptable quality and response times), and requirements for reporting, resolving, and terminating cloud services.

DOT Does Not Consistently Manage and Secure the Cloud Computing Resources for its Cloud-Based Systems

Nearly all the DOT cloud-based systems we examined have security weaknesses. Specifically, the Department does not consistently use secure configuration baselines, implement MFA to access its systems, encrypt data in transit or at rest, and keep software up to date with security patches for its OS and servers to protect its data and applications. According to NIST, the security of a fully virtual, cloud solution is heavily dependent on the individual security of each of its components, including the host[23] computer, OS, and applications.[24] DOT's weaknesses place its cloud-based systems' applications and data at risk of compromise.

We found that DOT and some OAs were not effectively managing and mitigating security and privacy control weaknesses for some of their cloud-based systems. Additionally, with the exception of FAA, FHWA, and FTA, DOT and its other OAs lack visibility into their CSP security weaknesses because they do not review their respective CSP continuous monitoring activities as required by FedRAMP. This has introduced security weaknesses into the systems.

[23] A host is any hardware device that has the capability of permitting access to a network via a user interface.
[24] NIST Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, January 2011.

We looked at selected cloud systems' security and privacy controls in the areas of configuration management, identity and access management, data protection and privacy, networking, applications, OS, and servers. We analyzed the systems' Security Assessment Reports, Plans of Action and Milestones (POA&Ms), and CSP FedRAMP Security Assessment Packages, including continuous monitoring activities. We also randomly selected for review 17 departmental cloud-based systems. For each of the 17 departmental cloud-based systems in our sample, we found system-specific security weaknesses where either DOT or the CSP were responsible for managing and protecting configuration management, identity and access management, data protection and privacy, networking, applications, OS, and servers. The following sections highlight key weaknesses for each of the 17 systems.

DOT Does Not Effectively Manage and Mitigate Security and Privacy Weaknesses for Its Cloud-Based Systems

Federal Motor Carrier Safety Administration (FMCSA)'s National Registry of Certified Medical Examiners—SaaS

FMCSA migrated its application-software National Registry of Certified Medical Examiners (NRCME) to its CSP's hybrid cloud. NRCME is a subsystem of FMCSA's Cloud Environment (CE) which has not completed a full security assessment since 2016. We found that this NRCME SaaS may be at risk of compromise. We identified weaknesses in four of the system computing resources under review—configuration management, identity and access management, data protection and privacy, and servers.

- The key weakness in NRCME is a subsystem of FMCSA's CE which has not had a completed security assessment since 2016. FMCSA security officials acknowledge FMCSA CE as having an exceptional amount of high-risk cybersecurity weaknesses, which we further discuss in detail below.

- Another major weakness appears to be FMCSA security officials' lack of visibility into the CSP's security weaknesses. The CSP is primarily responsible for managing and protecting networking, applications, OS, and servers, and has shared responsibility for identity and access management and data protection for SaaS. Thus, it's important for FMCSA security officials to be aware of risks the CSP's security weaknesses may introduce into the Agency's cloud-based system. We discuss this in detail in the following section.

- One weakness worth noting, among the others we will discuss in the next section, is that configuration setting issues with the CSP's server could allow a malicious actor to send erroneous data over the network and cause a denial-of-service attack.

FHWA's Mobile Solutions for Assessment and Report and Funds Tracking Module—SaaS

FHWA migrated its application hosting Mobile Solutions for Assessment and Report and Funds Tracking Module (MSAR & FTM) to its CSP's community cloud. Based on our review, the MSAR & FTM SaaS does not appear to be at risk of compromise.

- We did not identify any configuration management or identity and access management weaknesses. While we did identify other weaknesses with this SaaS, FHWA security officials provided evidence that they review the CSP's security weaknesses and appear to have taken the appropriate steps to mitigate the risks.

OST's Federal Human Resources Navigator—SaaS

OST migrated its Federal Human Resources Navigator (FHRN) tools for retirement to its CSP's community cloud. We found that the FHRN SaaS may be at risk of compromise. While we didn't identify any configuration management weakness, we did find weaknesses with identity and access management, data protection, and privacy.

- OST does not use personal identity verification (PIV) cards as the primary authentication mechanism to ensure secure login to the system.
- OST's FHRN collects personally identifiable information (PII) on employees but has not developed a Privacy Impact Analysis (PIA) to help identify and manage PII- and privacy-related risks.
- FHRN security officials have not identified anyone who can review the system's audit log files as required by DOT policy.
- FHRN security officials do not have a documented process to remove sensitive information from the information system within a 90-day timeframe in accordance with DOT requirements.

OST's Electronic Document Management System—SaaS

OST migrated its executive correspondence tracking services to its CSP's community cloud. OST's Electronic Document Management System (EDMS) SaaS may be at risk of compromise. While we didn't identify any configuration management weaknesses, we did find weaknesses with identity and access management and data protection.

- OST does not implement MFA for non-DOT system users who access its system, a key requirement for implementing ZTA.
- OST also does not ensure that inactive accounts are automatically disabled after 60 days as required for a moderate-impact system. DOT

policy[25] states that components are responsible for defining a time period for user account inactivity based on system categorization, and user accounts must be disabled after this time has elapsed.

- Without MFA and proper checks for inactive accounts, OST's EDMS faces increased risk that malicious actors may compromise accounts and gain unauthorized access, possibly resulting in data and system exploitation.

OST's Data Analysis Visualization Environment—SaaS
OST migrated its mapping and analytics application to its CSP's public cloud. OST's Data Analysis Visualization Environment (DAVE) SaaS may be at risk of compromise. We identified the following potential configuration management and data protection weakness:

- OST does not perform vulnerability scans of its cloud-based system on a monthly basis as required by DOT. Because OST security officials do not conduct vulnerability scanning to determine whether the system is properly configured or if security weaknesses exist or to address vulnerability results, they are placing their SaaS application and data at risk.

MARAD/US Merchant Marine Academy (MARAD/USMMA)'s Campus Labs —SaaS
MARAD migrated its student services application to its CSP's community cloud. MARAD/USMMA's Campus Labs SaaS has a high risk of being compromised. We identified weaknesses in all seven of the system computing resources under review—from configuration management to the servers.

- MARAD does not have a current security control assessment[26] and authorization in place. This leaves the system owner with limited assurance that security and privacy controls have been implemented effectively to protect the system.

- MARAD's security officials have issued a risk acceptance memo. However, they have not conducted the required security control assessment. As a result, security officials are unable to verify the current security posture and determine whether compensating security controls[27] are in place for their SaaS. This leaves the system at a high risk of compromise.

[25] DOT *Cybersecurity Compendium*, version 4.2, April 2018.

[26] A security control assessment determines the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome while meeting the security requirements for an information system or organization.

[27] The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization.

- MARAD has neither completed the required privacy threshold assessment (PTA) since fiscal year 2018 nor a PIA to protect the privacy and PII of its student information in the cloud.

FAA's Emergency Notification System—SaaS

FAA migrated its emergency notification services application to its CSP's community cloud. FAA's Emergency Notification System (ENS) SaaS does not appear to be at risk with one exception: a weakness with identity and access management.

- FAA's ENS security officials do not ensure that inactive accounts are automatically disabled after 90 days as required for a low-impact system.[28] FAA's ENS management has accepted the risk and per documented procedures, the enterprise and organizational administrators review the accounts of users frequently, and at least quarterly, which can allow them to disable accounts at that time. However, by not disabling accounts after 90 days, ENS security officials face the risk that a user who no longer needs access to the application can potentially still have access.

FRA's—Cloud Application Services SaaS

FRA migrated its grant management, attorney case management, and budget tracking services to its CSP's community cloud. FRA's SaaS may be at risk of compromise. We identified weaknesses for six of the seven system computing resources under review; the one exception was configuration management.

- The key weakness appears to be FRA security officials' lack of visibility into the CSP's security weaknesses. We discuss this in detail in the following section. However, we will highlight here a few weaknesses we identified with identity and access management, data protection, OS, and servers.
  - The CSP does not fully implement and enforce limited concurrent sessions that prevent multiple users from simultaneously logging onto the network with the same username and password.
  - The CSP uses obsolete software and OS; if exploited, they could allow an attacker to gain unauthorized access to the applications.
- FRA security and privacy officials need to update the PIA for one application, the Railroad Compliance System, to ensure the proper privacy controls are in place to protect sensitive information and PII. Without an

[28] DOT *Cybersecurity Compendium*, version 4.2, April 2018.

accurate PIA for its SaaS cloud-based system, FRA and its stakeholders may not know what types of data are being collected or stored.

NHTSA Web System—PaaS

NHTSA migrated its web-based content management system to use two CSP's public cloud. NHTSA's Web System (WS) PaaS may be at risk of compromise. We identified weaknesses for six of the seven system computing resources we reviewed; the one exception was the OS.

- A key weakness appears to be NHTSA security officials' lack of visibility into the CSP's security weaknesses, which hinders the CSP's ability to protect its network and OS.
    - The CSP's servers are not secure because its malicious code protection software is not adequate. This leaves the system open and vulnerable to the risk that malicious code will be introduced and cause data in transit and stored on servers to be exploited.
- NHTSA security officials did not complete weekly audit log reviews on the PaaS per the Agency's audit and accountability plan. As a result, NHTSA security officials may not be aware of various risks, including if the system is improperly configured or has existing software flaws.

NHTSA's Advanced Retrieval Tire, Equipment, Motor Vehicle, Information System—PaaS

NHTSA migrated its motor vehicle safety defects tracking system to use two CSP's public cloud. NHTSA's Advanced Retrieval Tire, Equipment, Motor Vehicle, Information System (ARTEMIS) PaaS may be at risk of compromise. We identified weaknesses for all seven of the system computing resources we reviewed—from configuration management to the OS.

- NHTSA security officials for ARTEMIS also lack visibility into both CSP's security weaknesses. This system has the same weaknesses as NHTSA WS, because they both use the same CSPs.
- NHTSA's PaaS lacks an updated PIA for determining the privacy risks associated with the PII data collected in ARTEMIS.

FTA's Transit Integrated Development Platform—PaaS

FTA migrated its financial and transit grant management platform to its CSP's hybrid cloud. FTA's Transit Integrated Development PaaS does not appear to be at risk of compromise. While we identified two security weaknesses in identity and access management and networking, FTA's security officials appear to be taking appropriate steps to address the risks.

- FTA security officials noted they are continuing to address residual risks dealing with non-enforced MFA for internal privileged and non-privileged network accounts and actions to bypass DOT's Trusted Internet Connection.[29]
- FTA has an open POA&M to track remediation of these vulnerabilities and continues to accept the associated risk.
- OIG currently has two open recommendations[30] to address these vulnerabilities.

PHMSA's Pipeline Risk Management Information System—IaaS and PHMSA Data Mart—IaaS

PHMSA migrated both of its disaster recovery services to the same CSP's public cloud. PHMSA Pipeline Risk Management Information System (PRIMIS) IaaS and PHMSA Data Mart (PDM) IaaS are both at risk of compromise. We identified weaknesses for six of the seven system computing resources we reviewed; the exception was configuration management.

- The key weakness appears to be PHMSA security officials' lack of visibility into both systems' CSP's security weaknesses. In particular, we identified unique weaknesses associated with identity and access management, data protection, OS, and servers that may introduce risks to both systems.
    - The CSP has not configured antivirus software with on-access scanning enabled. As a result, the software does not provide agencies with real-time scanning for cybersecurity threats or protection for their servers.
    - The CSP uses an obsolete OS for its web servers that has multiple vulnerabilities such as buffer overflow and potential remote execution.
    - The CSP lacks a mechanism for mitigating dynamic data link attacks that could prevent applications from running successfully.
    - The CSP does not fully implement and enforce limited concurrent sessions that prevent multiple users from simultaneously logging onto the network with the same username and password.
    - The CSP does not detect and prevent the unauthorized exfiltration of information across the interfaces it manages, and it has not

[29] OMB, *Updates to the Trusted Internet Connections (TIC) Initiative* (M-19-26), September 2019.

[30] *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.

implemented a means for PHMSA to monitor and analyze network traffic to detect and prevent unauthorized exfiltration.

  - The CSP does not monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions as required by FedRAMP.

FMCSA's Cloud Environment—IaaS

FMCSA migrated its enterprise system hosting services to its CSP's public cloud. FMCSA's CE IaaS is at a high risk of compromise. As previously noted for NRCME, FMCSA CE has not had a completed security assessment since 2016. We identified weaknesses in all seven of the system computing resources we reviewed—from configuration management to the servers.

- As FMCSA security officials noted in their ATO extension request, due to the legacy systems and applications in the cloud, an exceptional amount of high-risk cybersecurity weaknesses had been previously exposed. FMCSA CE security officials must address this high-risk weakness because CE hosts over 25 subsystems that provide licensing and insurance, drug and alcohol clearinghouse, and medical examiner registry services—all of which can be compromised.

- FMCSA security officials reported that to mitigate the impact of the Agency's cybersecurity weaknesses, they have instituted compensating controls. For example, they use a specific CSP because it is a FedRAMP-compliant cloud environment. However, FMCSA did not provide evidence that it had reviewed their CSP's continuous monitoring activities to ensure its cloud system security posture remains sufficient for the Agency's use as required by FedRAMP.

- Counter to DOT requirements, FMCSA lacks MFA for privileged and non-privileged network accounts; as a result, it faces the increased risk of compromised credentials and unauthorized access to its main IaaS.

- FMCSA security and privacy officials must update the Agency's PTA and PIA to protect the privacy of its users' PII and sensitive information.

FRA Multiple Cause Incident Analysis—IaaS

FRA migrated its analysis and decision support tool to its CSP's public cloud. FRA's Multiple Cause Incident Analysis (MCIA) may be at risk of compromise. We identified weaknesses in data protection and networking.

- A key weakness is FRA security officials' lack of visibility into the CSP's security weaknesses. We found that the CSP introduces risks to the system in data protection and networking. We highlight details of our findings and its impact on this system in the next section.

OST's Infrastructure and Operations Common Operating Environment (COE)—SaaS, PaaS, and IaaS

OST migrated its compute-as-a-service and disaster recovery services to its CSP's public cloud. We found that OST's COE SaaS, PaaS, and IaaS may be at risk of compromise. We identified weaknesses in all seven of the system computing resources we reviewed—from configuration management to the servers. It is important for OST security officials to address these weaknesses because the COE hosts cloud-based systems for other OAs, including FMCSA, FRA, NHTSA, and PHMSA and may introduce risks to those systems, as well.

- A key weakness is OST COE security officials' lack of visibility into the CSP's security weaknesses. We found that the CSP is introducing risks to the system.
- The lack of security baseline configuration settings and checklists introduces risks to network security due to a lack of visibility into software packages installed on servers, network components, and security patch software update information on the OS and applications.
- OST COE security officials do not review the system audit logs to enhance their ability to identify suspicious, inappropriate, unusual, or malevolent activity. As a result, the COE will not know if these activities present risks to the systems hosted within the IaaS environment.
- OST does not implement security patches to update software flaws in a timely manner. Its IaaS vulnerability scan results indicated several missing OS patches, and weekly vulnerability scans show missing security patches.
- The COE does not have a privacy plan in place and has not developed a PIA to determine how much PII it has to protect in the cloud environment for the OAs it serves. OST's COE security and privacy officials did not develop or complete the required PII inventory of applications and other capabilities for the IaaS environment. Due to the lack of a complete inventory, OST does not have the information it needs to complete the PIA. As a result, it could mislead the public about its IaaS operations and what is collected and stored with the environment.

FAA's Cloud Services—IaaS and PaaS

FAA migrated its server hosting services to its CSP's community cloud. We found that FAA's Cloud Services (FCS) IaaS and PaaS may be at risk of compromise. We identified weaknesses in all seven of the system computing resources we reviewed—from configuration management to the servers. It's important for FAA security officials to address these weaknesses because FCS hosts 13 cloud-based systems, some of which include PII. In addition, FCS weaknesses can introduce risks to the hosted systems, as well.

- FAA security officials did not incorporate flaw remediation into ongoing configuration management processes or regularly manage protections to detect and eradicate malicious code at entry points for the Agency's IaaS. As a result, they may unintentionally introduce malicious code to the system or cause system failure by failing to test software updates before installing them in the production environment.

- FAA's security officials did not implement a change control process, use baseline configuration settings, or document configuration settings. Without a baseline configuration process, FAA will not have a basis for future changes such as new software updates to the IaaS and PaaS.

- FAA security officials did not perform an automated review of network accounts or implement an alternative method for review. Since user accounts or credentials are the foundation for network security, this leaves FAA at risk for a data breach. Because FAA lacks an automated way to identify users on its network, an individual with an unauthorized account may access resources on the network without the Agency's knowledge.

- FAA did not monitor its IaaS communications traffic for unusual or unauthorized activities or conditions on inbound and outbound communication. We found that FCS security officials do not provide complete boundary protection and do not implement the most current cryptographic mechanisms to protect data during transmission.

- FAA security officials did not provide complete boundary protection or implement the most current cryptographic mechanisms to protect data during network transmissions. Due to the lack of boundary protection within the IaaS, FAA security officials may be unaware of all network traffic, putting the environment at risk of compromise.

- Data transmitted within the IaaS environment lacked encryption and is at risk of compromise and data exposure.

- The FCS system owner does not review vulnerability scans or conduct mitigation activities on its IaaS environment. Consequently, FAA may be unaware of potential vulnerabilities that put all systems housed in the IaaS environment at risk.

DOT Lacks the Necessary Visibility Into Its CSPs' Security Weaknesses, Leaving Its Cloud-Based Systems at Risk

We found that the security officials at DOT and most of its OAs—except for FAA, FHWA, and FTA—were not regularly reviewing their CSP's continuous monitoring activities for 13 of 17 systems in our sample. This activity should include reviewing the monthly POA&Ms, approving deviation requests and significant changes, and reviewing the results of the annual assessment. As a result, security officials cannot ensure their cloud system's security posture remains sufficient for their own use and supports ongoing authorization, as FedRAMP requires.

- Security officials for FMCSA, OST, MARAD, NHTSA, PHMSA, and FRA did not provide evidence that they had reviewed their CSP's continuous monitoring activities. As a result, they may not know whether their CSPs have security weaknesses that may introduce risks to their 13 cloud-based systems: FMCSA's NRCME and CE; OST's FHRN, EDMS, DAVE, and COE; MARAD's Campus Lab; FRA's Cloud Application Services and MCIA; NHTSA's WS and Artemis; and PHMSA's PRIMIS and PDM.
- Security officials for FAA, FHWA, and FTA reviewed their specific CSP's continuous monitoring activities and ensured the security posture for the other four cloud-based systems in our sample—FAA's ENS and FCS, FHWA's MSAR & FTM, and FTA's Transit Integrated Development Platform—remained sufficient for their use. They reviewed their respective CSP's security weaknesses, analyzed the risks, and considered the risks to be acceptable.

Security officials at DOT and its OAs must have visibility into their CSP's security weaknesses, since the responsibility for securing the SaaS offerings relies heavily upon the CSPs. In addition, the CSP share responsibility for managing and protecting the IaaS and PaaS cloud service offerings provisioned by DOT. During our analysis of CSP's continuous monitoring activities, we identified security weaknesses that DOT's CSPs could introduce in the following areas: data, network, application, OS, and servers. For example:

- Six sample systems that leverage two CSPs —FMCSA's CE, NHTSA's ARTEMIS, PHMSA's PDM and PRIMIS, FRA's MCIA, and OST's COE—have a data-related weakness. Specifically, the CSPs are using outdated versions of the Secure Sockets Layer/Transport Layer Security (SSL/TLS)[31] protocol, which have security weaknesses that may be exploitable. DOT requires OA servers to have updated SSL certificates to ensure the data transferred between the end user and the CSP's server remains private, and internet browser connections and transactions are secured by data encryption.
- Four systems that leverage a CSP—MARAD/USMMA's Campus Labs, PHMSA's PRIMIS and PDM, and OST's COE—have network-related weaknesses. Specifically, the CSP does not implement host-based firewalls on their physical servers, as FedRAMP requires, to help stop viruses and malicious software that may not be caught by network security. This also

[31] TLS is an authentication and encryption protocol widely implemented in browsers and web servers.

prevents the CSP from monitoring and controlling its incoming and outgoing network traffic. Lastly, the CSP is using an obsolete OS for one of its network devices which has multiple vulnerabilities.

- Four sample systems that leverage two CSPs—FAA's FCS, FMCSA's CE, and NHTSA's WS and ARTEMIS—have an application-related weakness. Each CSP does not provide malicious code protection for its physical servers. Therefore, the CSP's servers are not secure because the software application is not adequate, and the attack surface is open and vulnerable. Moreover, malicious code can be introduced to the server, which leaves data at rest and in transit at risk.

- The CSP, which is used by FMCSA's NRCME for commercial motor vehicle driver medical examination certifications and reports, has a server weakness. Specifically, the CSP, which is hosted on an IaaS, is vulnerable to a cross-site request forgery attack. This is a type of malicious exploitation of a website in which unauthorized commands are sent from a trusted user within the web application and may result in data theft.

- Four sample systems that leverage a CSP—OST's EDMS and COE and PHMSA's PRIMIS and PDM—have an OS-related weakness. Based on our review, this CSP uses obsolete and outdated software for the OS. This software does not have vendor support or security updates and can be exploited by malicious actors.

- Four sample systems that leverage a CSP—NHTSA's WS and ARTEMIS, FMCSA's CE, and FRA's MCIA—have network-related weaknesses. Specifically, the CSP does not support strict transport security. OMB Memo 15-13[32] requires Federal websites and services to enable Hypertext Transfer Protocol (HTTP) Strict Transport Security, which instructs compliant browsers to prevent information from being read or changed while in transit.

DOT Did Not Consistently Use the Appropriate Mechanisms To Deal With Cyberattacks on Its Cloud-Based Systems

DOT did not consistently use the appropriate mechanisms to detect, mitigate, and report cyberattacks on its cloud-based systems. For example, the Department's enterprise CSPs cloud services SLAs do not contain customized

[32] OMB, *Policy to Require Secure Connections across Federal Websites and Web Services (*M-15-13), June 2015.

language on reporting security incidents to the SOC as required by DOT's incident handling plan.[33] Also, DOT's SOC only monitors FAA's cloud-based systems for potential cybersecurity incidents and not the other OAs or the Department's cloud-based systems. Yet DOT's incident handling plan identifies the SOC as responsible for the daily cybersecurity incident collection, monitoring, tracking, management, and reporting for the Department's network and IT assets. Because the SOC does not monitor all departmental cloud-based systems as required, DOT and OA security officials may not be aware of potential security threats, and vulnerabilities may go undetected and unmitigated.

DOT's incident handling plan also states that SLAs and contracts with third-party service providers must provide related operational reporting, logging, and information. This is intended to facilitate the Department's complete situational awareness of the threats and vulnerabilities for information systems in its cloud environment. Additionally, all DOT's cloud SLAs must incorporate incident reporting requirements from their third-party service providers. However, the Department lacks security incident reporting for these SLAs, which in turn could potentially delay its required submission of cybersecurity incident reports to the Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT). If DOT's reports are delayed, the information stored on Federal cloud-based systems will be at risk of cyberattack because US-CERT is responsible for coordinating critical incidents with other Federal agencies.

DOT Lacks an Effective Strategy for Securing Its Cloud Services' Transition to ZTA

In May 2021, the President issued EO 14028, *Improving the Nation's Cybersecurity*, which initiated a sweeping effort to establish baseline security practices for migrating the Federal Government to ZTA, as well as realize the security benefits of cloud-based infrastructure while mitigating associated risks. The EO states that agencies should use cloud technology in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, migrations to cloud technology should adopt ZTA as practicable. To that end, the EO directed agencies to develop plans for implementing ZTA, adopt MFA, and encrypt data at rest and in transit.

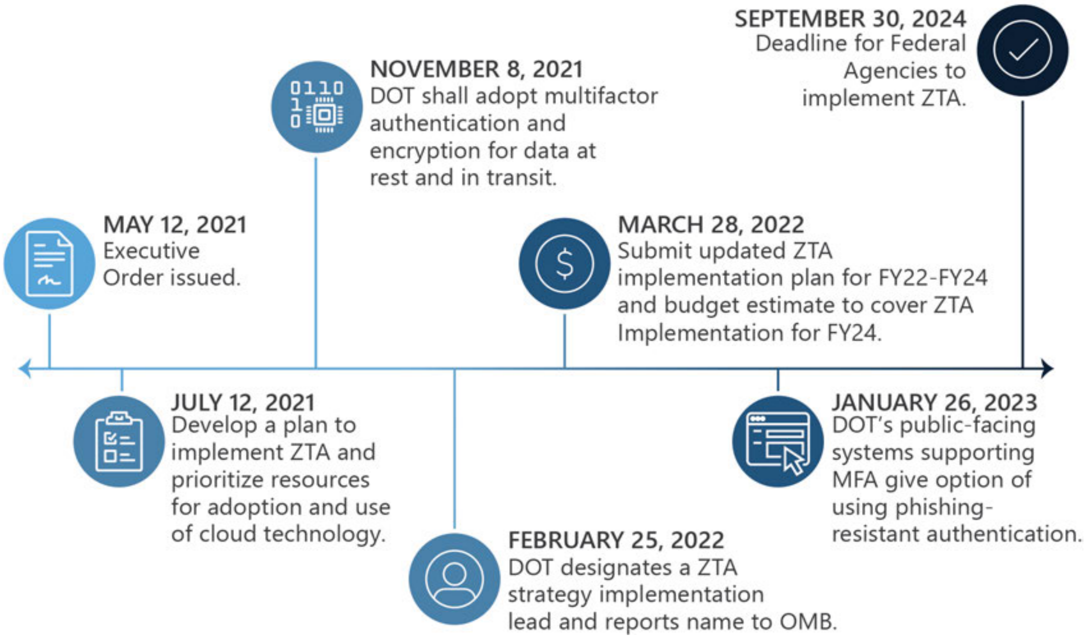
While the EO provided the initial requirements, in January 2022, OMB Memorandum M-22-09[34] established a Federal ZTA strategy that requires

[33] DOT, *Cybersecurity Incident Response Plan (IRP)*, version 3.1, July 2020.

[34] OMB, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (*M-22-09), January 2022.

agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024. The strategy reinforces the Government's defenses against increasingly sophisticated and persistent cybersecurity threats and details a number of key requirements, including designating a ZTA strategy implementation lead and submitting an updated ZTA implementation plan for fiscal years 2022–2024 with budget estimates (see figure 4).

Figure 4. Timeline of Key ZTA Implementation Requirements


MAY 12, 2021
Executive Order issued.
JULY 12, 2021
Develop a plan to implement ZTA and prioritize resources for adoption and use of cloud technology.
NOVEMBER 8, 2021
DOT shall adopt multifactor authentication and encryption for data at rest and in transit.
FEBRUARY 25, 2022
DOT designates a ZTA strategy implementation lead and reports name to OMB.
MARCH 28, 2022
Submit updated ZTA implementation plan for FY22-FY24 and budget estimate to cover ZTA Implementation for FY24.
JANUARY 26, 2023
DOT's public-facing systems supporting MFA give option of using phishing-resistant authentication.
SEPTEMBER 30, 2024
Deadline for Federal Agencies to implement ZTA.

Source: OIG analysis of EO 14028 and OMB M-22-09

DOT has taken a number of steps, such as designating a ZTA implementation lead and submitting its initial plan to implement ZTA. While the plan included steps for FAA's migration and implementation to ZTA, it lacked appropriate information regarding DOT's migration steps to implement ZTA. The EO required agencies to develop a plan to implement ZTA and incorporate, as appropriate, the migration steps that NIST have outlined in standards and guidance, describe any steps that have already been completed, and include a schedule to implement them. Specifically, DOT's plan does not have a proposed implementation schedule for most of the OAs—the exception is FAA.

Furthermore, DOT has yet to complete two of the five key EO and OMB milestones required to be met by this point in time (see table). For example, DOT has yet to fully adopt MFA and encryption for data at rest and in transit Departmentwide. DOT has submitted an updated ZTA implementation plan and reported to OMB that it has identified the necessary resources required to deploy ZTA in a timely manner. However, DOT stated that implementation depends on successful allocation of funding to support the EO requirements. Finally, the updated plan includes a scheduled completion date of fiscal year 2026 for DOT, and fiscal year 2028 for FAA, while the current OMB deadline is the end of fiscal year 2024.

Table. Status of Key Milestones for DOT's ZTA Implementation

Responsibility	Description	Current Status
Prioritize resources for the adoption and use of cloud technology	Within 60 days of EO 14028, update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance.	Complete
Submit initial ZTA implementation plan	Within 60 days of EO 14028, develop a plan to implement ZTA, which shall incorporate, as appropriate, the migration steps that NIST within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them.	Complete
Adopt MFA and encryption for data at rest and transit	Within 180 days of EO 14028, agencies shall adopt MFA and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. Submit progress reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the Assistant to the President and National Security Advisor every 60 days until DOT fully adopts agency-wide MFA and data encryption.	In progress
Designate a ZTA strategy implementation lead	Agencies will have 30 days from the publication of OMB Memorandum M-22-09 to designate and identify a zero trust strategy implementation lead for their organization. OMB will rely on these designated leads for Governmentwide coordination and for engagement on planning and implementation efforts within each organization.	Complete
Submit revised ZTA implementation plan along with FY 2024 budget request	Within 60 days of the date of this memorandum, agencies must build upon those plans by incorporating the additional requirements identified in this document and submitting to OMB and CISA an implementation plan for FY 2022–2024 for OMB concurrence, and a budget estimate for FY 2024.	In progress

Source: OIG analysis

The zero trust initiative is a dramatic paradigm shift in the Federal Government's cybersecurity philosophy regarding the security of infrastructure, networks, and data. Previously, agencies verified users, devices, applications, and transactions once they arrived at the network perimeter. With ZTA, agencies must continually verify each user, device, application, and transaction. Without a complete implementation plan or strategy for adopting ZTA, DOT may not be able to meet the key milestones outlined in the EO and OMB memorandum and implement ZTA by OMB's deadline.

Conclusion

Federal agencies must follow cybersecurity policy, ensure network security, and successfully implement cloud technologies while protecting data stored in the cloud from malicious actors. DOT has taken action to continue its migration to cloud-based solutions and modernize its IT infrastructure. However, it has not developed specific cloud services policies and procedures or a governance process that enforces the Department's adherence to all applicable Federal guidelines for cloud services. Further, DOT has not ensured that baseline security practices are in place to migrate to a zero trust architecture and to realize the security benefits of a cloud-based infrastructure. Until the Department does so, it will be hindered in its ability to meet the administration's goal to modernize Federal Government cybersecurity by accelerating the movement to secure cloud services, adopting security best practices, and advancing toward zero trust architecture.

Recommendations

To improve the Department's cloud services program and transition its enterprise network to zero trust architecture, we recommend that DOT's Chief Information Officer:

1. Develop and implement policies and procedures governing DOT components and Operating Administrations' adoption and use of cloud services for their cloud-based system and at a minimum require system owners to:

    a. Submit an Authorization to Operate letter to the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office before adopting and using cloud services to ensure (1) cloud services comply with FedRAMP security baselines, and (2) FedRAMP has an accurate inventory of DOT cloud services and cloud service providers.

    b. Conduct a quality and risk review of the Department's cloud service providers cloud service offering authorization package to ensure that it clearly and accurately reflects the cloud service offering's security posture so DOT's Authorizing Official can make an informed risk-based authorization decision, as required by FedRAMP.

    c. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of the respective cloud service providers' continuous monitoring activities to ensure their cloud systems' security posture remains sufficient for their own use and supports ongoing authorization, as required by FedRAMP.

2. Incorporate the required standard cloud security clauses in the Department's enterprise cloud service contracts as well as other cloud services contracts for FAA, MARAD, and OST to ensure the cloud services are secure.

3. Working with the appropriate DOT procurement officials for FAA, FMCSA, FHWA, MARAD, FRA, NHTSA, PHMSA, and OST, set up service level agreements as required, with each of their cloud service providers to define and set agency expectations and cloud service provider-specific responsibilities.

4. Direct and require confirmation of completion from FMCSA's cloud-based system owners for the National Registry of Certified Medical Examiners—Software-as-a-Service to include in its Executive Summary/Authorization to Operate Letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

5. Direct and require confirmation of completion from OST's cloud-based system owner for the Federal Human Resources Navigator—Software-as-a-Service to:

   a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

   b. Use personal identity verification cards as the primary authentication mechanism to ensure secure system login.

   c. Develop a Privacy Impact Analysis to help identify and manage personally identifiable information and privacy risks.

   d. Identify a security official to review system audit log files.

   e. Develop and implement a process to remove extracted data containing sensitive information within 90 days of extraction in accordance with DOT requirements.

6. Direct and require confirmation of completion from OST's cloud-based system owner for the Electronic Document Management System—Software-as-a-Service to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Require multifactor authentication for non-DOT system users.

    c. Develop and implement a process to automatically disable inactive system accounts after 60 days of inactivity.

7. Direct and require confirmation of completion from OST's cloud-based system owner for the Data Analysis Visualization Environment—Software-as-a-Service to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Develop and implement a process to conduct monthly vulnerability scans as required by DOT.

8. Direct and require confirmation of completion from MARAD's cloud-based system owner for US Merchant Marine Academy/Campus Labs—Software-as-a-Service to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Complete an annual security authorization process and obtain a full Authorization to Operate for its Software-as-a-Service cloud information system to ensure all system risks have been properly identified and accepted in accordance with departmental cybersecurity policies.

c. Update its privacy threshold assessment and, if applicable, Privacy Impact Analysis to protect privacy, personally identifiable information, and other sensitive information stored in the cloud.

9. Direct FAA's cloud-based system owner for the Emergency Notification System—Software-as-a-Service to provide evidence of the organizational administrator's quarterly reviews of Emergency Notification System application and documentation verifying they disable inactive accounts.

10. Direct and require confirmation of completion from FRA's cloud-based system owner for its Cloud Application Services—Software-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Update the Privacy Impact Analysis for the Railroad Compliance System to ensure the proper privacy controls are in place to identify and protect personally identifiable information and other sensitive information.

11. Direct and require confirmation of completion from NHTSA's cloud-based system owner for the Web System—Platform-as-a-Service and Infrastructure-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Develop and implement a process to review audit logs and analyze vulnerability scan reports on its Platform-as-a-Service on a weekly basis to check for various risks, including software flaws per NHTSA's audit and accountability plan.

12. Direct and require confirmation of completion from NHTSA's cloud-based system owner for the Advanced Retrieval Tire, Equipment, Motor Vehicle, Information System—Platform-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP

b. Update the Privacy Impact Analysis to ensure the proper privacy controls are in place to identify and protect personally identifiable information and other sensitive information.

13. Direct and require confirmation of completion from PHMSA's cloud-based system owner for the Pipeline Risk Management Information System—Infrastructure-as-a-Service—and PHMSA Data Mart—Infrastructure-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization as FedRAMP requires for the Pipeline Risk Management Information System.

    b. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization as FedRAMP requires for PHMSA Data Mart.

14. Direct and require confirmation of completion from FMCSA's cloud-based system owner for the Cloud Environment—Infrastructure-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use as required by FedRAMP.

    b. Complete its annual security authorization process and obtain a full Authorization to Operate for its cloud information system to ensure all system risks have been properly identified and accepted in accordance with departmental cybersecurity policies.

    c. Develop and implement a process to enforce multifactor authentication for privileged and non-privileged network accounts.

    d. Update the privacy threshold assessment and Privacy Impact Analysis to protect the privacy of its system users' personally identifiable information and other sensitive information.

15. Direct and require confirmation of completion from FRA's cloud-based system owner for the Multiple Case Incident Analysis—Infrastructure-as-a-Service—to include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its review of cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

16. Direct and require confirmation of completion from OST's cloud-based system owner for the Infrastructure and Operations Common Operating Environment (COE)—Software-as-a-Service, Infrastructure-as-a-Service, and Platform-as-a-Service—to:

    a. Include in its executive summary/Authorization to Operate letter to the Authorizing Official proof of its cloud service provider's continuous monitoring activities to ensure its cloud system security posture remains sufficient for its own use and supports its ongoing authorization, as required by FedRAMP.

    b. Develop security baseline configuration settings and a checklist and assess whether the COE cloud-based system is properly configured and the network secure.

    c. Develop and implement a process to conduct reviews of the system audit logs to enhance its ability to identify suspicious, inappropriate, unusual, or malevolent activity.

    d. Develop and implement a process that requires timely updates to security patches that address software flaws which mitigate the risks associated with mission-related operating system patches and data exfiltration.

    e. Develop a Privacy Impact Analysis to identify and protect personally identifiable information and other sensitive information hosted in the COE cloud.

17. Direct and require confirmation of completion from FAA's cloud-based system owner for the FAA Cloud Services—Infrastructure-as-a-Service and Platform-as-a-Service—to:

    a. Incorporate flaw remediation into ongoing configuration management processes.

    b. Develop and implement a process to regularly manage malicious code protection to detect and eradicate malicious code at the entry point for its Infrastructure-as-a-Service and Platform-as-a-Service.

c. Develop and implement a change control process and use baseline configuration settings and document configuration settings to establish a basis for future builds, releases, and/or changes.

d. Develop and implement a process to perform an automated review of network accounts or implement an alternative method for identifying users on the network in real-time.

e. Develop and implement a process to require the most current cryptographic mechanisms to protect data during network transmission to provide complete boundary protection and reduce the risk of compromise.

f. Develop and implement a process to encrypt data transmitted within the Infrastructure-as-a-Service environment to reduce the risk of compromise and data exposure.

g. Develop and implement a process to review vulnerability scans results and remediate vulnerabilities within specified timeframes as required by FAA's security handbook.

18. Direct departmental security officials working with appropriate procurement officials to verify that service level agreements contain a requirement to report security incidents to DOT's Security Operations Center and require confirmation of completion.

19. Develop and implement a process that enables FAA's Security Operations Center to receive the necessary log data for ensuring proper cybersecurity incident monitoring for all departmental cloud-based systems.

20. Report DOT plans for fully adopting multifactor authentication and encryption for data at rest and in transit in accordance with Executive Order 14028.

21. Update the Department's zero trust architecture strategy and implementation plan to address the identified gaps and include migration steps and timelines consistent with direction from the Office of Management and Budget and National Institute of Standards and Technology guidelines.

Agency Comments and OIG Response

We provided DOT with our draft report on April 25, 2023, and received its formal response on July 19, 2023. DOT's response is included in its entirety as an appendix to this report. DOT fully concurred with recommendations 1,9,17, and 19–21 and provided appropriate planned actions and completion dates. DOT concurred with our intent for recommendations 2–8, 10, 12–14, 16 and 18 and proposed appropriate alternative actions and completion dates for all except recommendations 2 and 3. DOT requested we close recommendation 11 and did not concur with recommendation 15.

For recommendations 2 and 3, we understand the Department's request that we issue separate recommendations directly to FAA for addressing relevant actions within FAA contracts. However, we believe that the Department's Chief Information Officer and OCIO have the authority to direct FAA to take the relevant actions.

The Department requested we close recommendation 11 upon issuance of the final report, because NHTSA completed actions to address our findings in October 2022. We will consider closing the recommendation upon receiving supporting documentation to review and verify whether NHTSA has taken the appropriate actions to meet the intent of our recommendation.

We ask the Department to reconsider its position for recommendation 15. The Department reported it provided evidence of authorization and continuous monitoring activities for the Multiple Case Incident Analysis[35] system. FRA reported it received no questions or findings regarding the sufficiency of or weaknesses with FRA's documentation processes. However, while we discussed and reported to FRA officials that its authorization activities did provide evidence of performing an annual assessment of its CSP's continuous monitoring activities, they did not provide evidence of continuous monitoring on a monthly basis as required by FedRAMP. We believe if FRA agrees to implement the Department's proposed alternative actions for recommendations requesting DOT to update its Authority to Operate letters, FRA will meet the intent of this recommendation.

[35] The proper name for this system is Multiple Cause Incident Analysis.

Actions Required

We consider recommendations 1, 4–10, 12–14, and 16–21 resolved but open pending the completion of the planned actions. We request that DOT provide an updated response on its plans to address relevant actions within FAA contracts for recommendation 2 and 3, provide documentation to support closing recommendation 11, and reconsider its position regarding recommendation 15. In accordance with DOT Order 8000.1C, we request that DOT provide its revised response within 30 days of the date of this report.

Exhibit A. Scope and Methodology

This performance audit was conducted between November 2021 and April 2023. We conducted this audit 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. Our audit objectives for this self-initiated audit were to assess the effectiveness of the Department's cloud systems' security and privacy controls and the strategy to secure cloud services in order to implement ZTA.

To assess the security and privacy controls for the Department's cloud systems, we obtained a listing of CSPs, and the associated systems used by the Department and OAs. We worked with OIG's statistician team to generate our initial sample universe. When applicable, we randomly selected one moderate risk and one high risk system from each OA. If an OA did not have at least one of each system, we randomly sampled two high risk or two moderate risk systems. Some OAs only had one system, so in those cases we had one option for selection. Additionally, we randomly sampled two low-impact SaaS systems out of the seven across the OAs. As a result, our initial sample included a total of 20 systems (6 high risk, 12 moderate risk, and 2 low risk). If available, we also pulled alternate systems for each OA in case one system needed to be substituted out for auditing purposes. We removed any cloud service offering that was not associated with a DOT information system, generating our final universe of 17 systems. We reviewed a selection of security controls based on the system computing resources identified in CISA's Cloud Security Technical Reference Architecture. Additionally, we reviewed system security documentation for our sample, including system categorization documents, system security plans, security assessment reports, POA&Ms, and Executive Summaries. We also collected and analyzed relevant data pertaining to DOT's internal controls for identifying cloud services, available contracts, and service-level agreements associated with CSPs. Moreover, we met with DOT officials to gain an understanding of the support the Department provides to the OAs for cloud services. We also met with the FedRAMP Acting Director to gain an understanding of their oversight and governance responsibilities for Governmentwide CSPs and associated cloud service offerings. We reviewed continuous monitoring reports for the associated CSPs to determine what risks have not been mitigated that could potentially be inherited by DOT and its OAs. We reviewed OIG open recommendations pertaining to the Department's cloud services program to determine whether corrective actions have been taken.

To assess the Department’s strategy to secure cloud services to implement ZTA, we collected and analyzed DOT’s submissions to OMB in support of Executive Order 14028 and OMB Memo 22-09. We determined whether DOT was meeting the requirements from Executive Order 14028, which directs Federal departments and agencies to make significant contributions toward modernizing cybersecurity defenses by protecting Federal networks; and OMB M-22-09, which sets forth a Federal ZTA strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024.

In addition, we met with DOT officials to gain an understanding of their plan submission and progress made for the implementation of ZTA.

Exhibit B. Organizations Visited or Contacted

Federal Aviation Administration

Federal Highway Administration

Federal Motor Carrier Safety Administration

Federal Railroad Administration

Federal Transit Administration

Maritime Administration

National Highway Traffic Safety Administration

Office of the Chief Information Officer

Office of Inspector General

Office of the Secretary of Transportation

Pipeline and Hazardous Materials Safety Administration

Exhibit C. List of Acronyms

ARTEMIS	Advanced Retrieval Tire, Equipment, Motor Vehicle, Information System
ATO	Authorization to Operate
CE	Cloud Environment
CISA	Cybersecurity Infrastructure Security Agency
COE	Common Operating Environment
CSO	Cloud Service Offering
CSP	Cloud Service Provider
DAVE	Data Analysis Visualization Environment
DOT	Department of Transportation
EDMS	Electronic Document Management System
ENS	Emergency Notification System
EO	Executive Order
FAA	Federal Aviation Administration
FCS	FAA Cloud Services
FedRAMP	Federal Risk and Authorization Management Program
FHRN	Federal Human Resource Navigator
FHWA	Federal Highway Administration
FISMA	Federal Information Security Modernization Act
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure-as-a-Service
IT	Information Technology
MARAD	Maritime Administration
MCIA	Multiple Cause Incident Analysis
MFA	Multifactor Authentication

MSAR & FTM	Mobile Solutions for Assessment and Report and Funds Tracking Module
NHTSA	National Highway Safety Administration
NIST	National Institute of Standards and Technology
NRCME	National Registry of Certified Medical Examiners
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Operating System
OST	Office of the Secretary
PaaS	Platform-as-a-Service
PHMSA	Pipeline and Hazardous Materials Safety Administration
PDM	PHMSA Data Mart
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PMO	Program Management Office
POA&M	Plans of Action and Milestones
PRIMIS	Pipeline Risk Management Information System
PTA	Privacy Threshold Assessment
SaaS	Software-as-a-Service
SLA	Service Level Agreements
SOC	Security Operations Center
SSL	Secure Sockets Layer
TIC	Trusted Internet Connection
TLS	Transport Layer Security
USMMA	U.S Merchant Marine Academy
US-CERT	U.S. Computer Emergency Response Team
WAN	Wide Area Network

WS	Web System
ZTA	Zero Trust Architecture

Exhibit D. Presence of Security Weaknesses in DOT Cloud-Based Systems

CUI	CUI	CUI	CUI	CUI	CUI	CUI	CUI
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

CUI [redacted]	CUI [redacted]	CUI [redacted]	CUI [redacted]	CUI [redacted]	CUI [redacted]	CUI [redacted]	CUI [redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

CUI [redacted]

Exhibit E. Major Contributors to This Report

NATHAN CUSTER	PROGRAM DIRECTOR
STACY JORDAN	PROGRAM DIRECTOR
SHAVON MOORE	SENIOR IT SPECIALIST
NELSON FLORES	SENIOR IT SPECIALIST
THADDEUS PATRICE, JR	IT SPECIALIST
JANE LUSAKA	SENIOR WRITER-EDITOR
SUSAN CROOK-WILSON	WRITER-EDITOR
MORGAN ATHERTON	WRITER-EDITOR
TOM DENOMME	CONSULTANT
CELESTE VERCHOTA	ASSOCIATE COUNSEL
CHELSEA ARLANTICO	ASSOCIATE COUNSEL
GEORGE ZIPF	SENIOR STATISTICIAN
GRACE ENTWISTLE	STATISTICIAN

Appendix. Agency Comments

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

Memorandum

Subject: INFORMATION: Management Response to Office of Inspector General (OIG) Draft Report on DOT Cloud Services

From: Cordell Schachter
DOT Chief Information Officer

CORDELL SCHACHTER

Digitally signed by CORDELL SCHACHTER
Date: 2023.07.19 16:01:31 -04'00'

To: Kevin Dorsey
Assistant Inspector General for IT Audits

The Department of Transportation (DOT or Department) continues to prioritize cybersecurity and full implementation of cloud technologies and solutions while ensuring the protection and security of agency networks and data. As part of those efforts, the Office of the Chief Information Officer (OCIO) has formed a cross-functional workgroup to conduct a review of the current cloud-based solutions. OCIO plans to publish an Information Technology (IT) Cloud Plan by the end of fiscal year 2023 that details requirements, procedures, and resources available within the DOT IT community to ensure cloud services and modernized IT infrastructure based on security best practices and the agency's zero trust architecture.

Upon review of OIG's draft report, the Department concurs with recommendations 1-10, 11-14, and 16-21, and non-concurs with recommendation 15. A detailed chart of implementation dates for all recommendations is listed at the end of this document.

For the recommendations requesting DOT to update its Authority to Operate (ATO) letters (recommendations 4-6, 8, 12-14, 16), we propose an alternate action whereby DOT updates the Security Authorization and Continuous Monitoring Performance Guide (current revision v 4.2) with the necessary direction and required language. ATO letters will be in alignment with the updated requirements in the Guide. At the time of review by OIG, the systems were properly authorized per DOT guidance in effect at the time of authorization. Requiring ATO letters to be updated out of the cycle will require additional resources of the agency without a significant return on value from the related work. The proposed action will enhance the security of the IT portfolio. As an additional benefit, the efficacy of the DOT-selected controls can be evaluated during a future FISMA evaluation cycle.

For recommendation 2, the Department concurs with OIG's intent; however, we propose alternative actions. We propose to leverage actions performed in response to Recommendation 18 and coordinate the implementation of modifications to the Departmental Enterprise, Maritime Administration, and Office of the Secretary (OST) cloud contracts with the appropriate acquisition officials. Actions to implement this alternative solution will be completed by December 30, 2023. Given the Federal Aviation Administration's (FAA) separate statutory authorities under its Acquisition Management System (AMS), we recommend that OIG issue a separate recommendation directly to FAA to address relevant actions within FAA contracts.

For recommendation 3, the Department concurs with OIG's intent; however, we propose alternative actions. As noted during the audit, the services provided by the cloud providers are governed by the terms and conditions and service levels associated with the provided services for the respective communities of customers and are not separately modifiable or negotiable by the government. The provided service levels are typically incorporated into the award conditions and may only be negotiable under limited conditions. We propose to coordinate with the Office of the Senior Procurement Executive to develop an acquisition directive explaining how service-level agreements work in cloud environments and citing when a service-level agreement should be included. Actions to implement this alternative solution will be completed by December 30, 2023. Given FAA's separate statutory authorities under its AMS, we recommend that OIG issue a separate recommendation directly to FAA to address similar findings within FAA contracts.

For recommendation 6, although we concur to implement the recommendation, we would like to note that the DOT Information Technology Implementation Memorandum ITIM-2022-006 dated July 2022 requires multifactor authentication for non-DOT system users. We will enforce this existing requirement.

For recommendation 7, the Department concurs with OIG's intent; however, we propose alternative actions. Departmental records and vulnerability assessment reports substantiate that the Data Analysis Visualization Environment has been authorized and undergoing continuous monitoring, including a review of the cloud service providers' continuous monitoring data, in accordance with the Department's Security Authorization and Continuous Monitoring Performance Guide (SACMPG) since the system's inception in 2018, and scanned monthly for vulnerabilities by the Department's enterprise vulnerability scanning capability since at least April 2021. The system is currently undergoing a reauthorization during which the system configuration, controls and monitoring are revalidated, and documentation is updated. We propose to address any identified weaknesses in accordance with the SACMPG, creating POAMs (plan of action and milestones) by December 30, 2023, and addressing remediation and mitigation in accordance with DOT's published requirements by December 30, 2024.

For Recommendation 10, the Department concurs with the OIG's intent; however, we propose alternative action. The second part of the recommendation references the Federal Railroad Compliance System (RCS), which does not exist as a separate system in the Department's system inventory, and the privacy risk of which is managed under the Federal Railroad Administration's (FRA) Cloud Application Services system as evidenced in that system's Privacy Threshold Analysis. We propose to address the identified issue in accordance with the

Departmental Privacy Risk Management policy and guidance by updating the Privacy Impact Assessment for RCS' parent system, the FRA Cloud Application Services system.

For Recommendation 15, the Department does not concur. The Department provided evidence of authorization and continuous monitoring activities for the Multiple Case Incident Analysis systems and received no questions or findings regarding the sufficiency of or weaknesses within FRA's documentation and processes. We request OIG close this recommendation upon issuance of the final report.

For recommendation 11, the National Highway Traffic Safety Administration completed actions to address OIG's findings in October 2022. We request OIG close this recommendation upon issuance of the final report.

For Recommendation 18, the Department concurs with OIG's intent; however, we propose alternative action. Incident reporting and communication requirements are already established in the Department's Transportation Acquisition Regulation (TAR) clauses 1239.7002[1] and 1252.239-76[2], and General Services Administration's FedRAMP incident reporting requirements as published in the FedRAMP control specific contract clauses[3] and baseline control requirements[4] for the incident response (IR) control family. We propose, instead, to coordinate with the Office of the Senior Procurement Executive to develop and issue guidance clarifying the distinctions between contracts and service-level agreements, and where and when to use each, and reinforcing prior direction on the inclusion of the IT-related TAR clauses into agency contracts under appropriate conditions. Actions to implement this alternative solution will be completed by December 30, 2023.

Recommendations	Concur Status	Implementation Dates
1, 4-6, 8, 9, 12-14, 16, 17, 19-20	Concur	September 30, 2023
21	Concur	December 30, 2024
2, 3, 10, 18	Concur with Alternate Action	December 30, 2023
7	Concur with Alternate Action	December 30, 2024
15	Non-Concur/Request Closure	N/A
11	Concur/Request Closure	N/A

[1] Transportation Acquisition Regulation (TAR) 1239.7002, *Information Security and Incident Response Reporting – Policy*, https://www.acquisition.gov/tar/part-1239-acquisition-information-technology

[2] Transportation Acquisition Regulation (TAR) 1239.252-76, *Cloud Computing Services*, https://www.acquisition.gov/tar/part-1239-acquisition-information-technology

[3] FedRAMP Control Specific Clauses; December 8, 2017; https://www.fedramp.gov/assets/resources/documents/Agency_Control_Specific_Contract_Clauses.pdf

[4] FedRAMP Moderate Authorization Toolkit, https://www.fedramp.gov/assets/resources/toolkits/FedRAMP-Moderate-Authorization-Toolkit.zip

U.S. Department of Transportation
Office of Inspector General

Fraud, Waste, & Abuse Hotline

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

OUR MISSION

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

OFFICE OF INSPECTOR GENERAL • U.S. DEPARTMENT OF TRANSPORTATION •

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