FTA

Report IT2022005
October 20, 2021

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

FOR OFFICIAL USE ONLY

Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552.

U.S. Department of Transportation
Office of Inspector General

Highlights

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

Self-Initiated

Federal Transit Administration | IT2022005 | October 20, 2021

What We Looked At

The Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 set up appropriations to support executive agency operations during the COVID-19 pandemic. The Federal Transit Administration (FTA) has received nearly $70 billion in CARES Act and other COVID-19 relief appropriations. FTA uses several financial management systems to approve, process, and disperse this funding for the transit industry's COVID-19 response and recovery. Given the size of this investment, we initiated this audit. Our audit objective was to assess the effectiveness of FTA's financial management systems' security controls designed to protect the confidentiality, integrity, and availability of the systems and their information.

What We Found

FTA's financial management systems have security control deficiencies that could affect FTA's ability to approve, process, and disburse COVID-19 funds. FTA security officials mislabeled and incorrectly documented control types for over 180 security controls in its fiscal year 2020 system security plans for these systems. FTA also does not adequately monitor security controls provided by or inherited from DOT's common control provider [redacted] FTA also has not remediated security control weaknesses identified since 2016. If compromised, these weaknesses could allow a cybersecurity attack. [redacted] ue to these security control weaknesses, FTA's security officials cannot be sure financial management systems have the proper safeguards and countermeasures in place to protect the systems and that they effectively manage information security risk.

Our Recommendations

FTA concurred with all of our 13 recommendations to help the Agency address its security control weaknesses and improve its systems' cybersecurity posture.

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.

FOR OFFICIAL USE ONLY

Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552.

Contents

U.S. Department of Transportation
Office of Inspector General

Memorandum

Date: October 20, 2021

Subject: ACTION: 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 | Report No. IT2022005

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Federal Transit Administrator

The United States transportation system facilitates the Nation's jobs, businesses, and way of life. The transportation industry has been one of the hardest hit by the Coronavirus Disease 2019 (COVID-19) pandemic. In March 2020, the President signed the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[1] This law, in part, set up appropriations to support executive branch agency operations during the pandemic.

The Department of Transportation (DOT) received over $36 billion in CARES Act funds, and from that amount, the Federal Transit Administration (FTA) received $25 billion. The act appropriated funds to FTA for Transit Infrastructure Grants to prevent, prepare for, and respond to the pandemic. FTA has received additional COVID-19 funds, increasing its total to nearly $70 billion.[2] FTA uses several financial management systems to approve, process, and disperse the funding it provides to support the transit industry's COVID-19 response and recovery efforts.

FTA's application of information security controls and recovery procedures to the financial management systems it uses to approve, process, and disperse COVID-19 funds can protect these systems from malicious actors and system failure. Given the size of these COVID-19 related investments, we initiated this audit. Our audit objective was to assess the effectiveness of FTA's financial management

[1] Coronavirus Aid, Relief, and Economic Security (CARES) Act, Pub. L. No. 116-136, 2020.

[2] Coronavirus Response and Relief Supplemental Appropriations Act, Pub. L. 116-123, 2020; American Rescue Plan Act, Pub. L. 117-2, 2021.

systems' security controls[3] designed to protect the confidentiality,[4] integrity,[5] and availability[6] of the systems and their information.

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

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1518, or Nathan Custer, Program Director, at (202) 366-5540.

cc: The Secretary
DOT Audit Liaison, M-1
Federal Transit Administration Audit Liaison, TBP-31

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

[4] Confidentiality refers to maintaining restrictions on information access and disclosure that protect individual privacy and proprietary information.

[5] Integrity refers to guarding against improper modification or destruction of information.

[6] Availability refers to maintaining timely and reliable access to and use of information.

Results in Brief

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.

FTA's financial management systems have several security control deficiencies that could affect the Agency's ability to approve, process, and disperse COVID-19 funds. For example, FTA security officials mislabeled and incorrectly documented the wrong control type for over 180 security controls in its fiscal year 2020 system security plans (SSP)[7] for its financial management systems. This mislabeling creates the question whether the individual responsible for testing each system's controls was the system owner or common control provider. FTA also does not adequately monitor the security controls provided by or inherited from DOT's common control provider.[8] For example, we found 139 of 269 security controls inherited that were not tested or implemented but reported as satisfied by FTA officials. [redacted], increasing FTA's financial management systems' exposure to outside threats. Additionally, FTA has not remediated longstanding security control weaknesses that it has identified since 2016, that if compromised, could lead to a cybersecurity attack. For example, [redacted] Moreover, [redacted] Furthermore, FTA lacks effective contingency planning and incident response capabilities such as identifying an alternate set of personnel to restore its financial management systems if primary contingency personnel are unavailable. [redacted]. Given the number and significance of these security control weaknesses, FTA's security officials cannot be sure the Agency's financial management systems have the proper safeguards and

[7] A system security plan provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

[8] This common control provider is DOT's IT Shared Services' (ITSS) common operating environment (COE), a Government-owned, contractor developed and supported, general support system that provides DOT's Operating Administrations (OA) with information technology services.

[9] A software patch is software used to correct problems, frequently pertaining to security issues, in operating systems and software programs.

countermeasures in place to protect its systems and that they are effectively managing information security risk.

We made 13 recommendations to address FTA's security control weaknesses and help improve the cybersecurity posture of the Agency's financial management systems. FTA has concurred with all 13 recommendations.

Background

FTA provides financial and technical assistance for public transportation systems including bus, subway, light rail, commuter rail, trolley, and ferry systems. It also oversees safety measures and helps conduct technology research. The Agency is comprised of 10 regional offices that assist transit agencies in all 50 States, the District of Columbia, and U.S. territories.

FTA oversees grants to State and local transit providers primarily through its 10 regional offices. These recipients are responsible for managing their programs in compliance with Federal requirements. FTA is responsible for ensuring that recipients follow Federal requirements. Additionally, FTA evaluates recipient compliance through its oversight program, which requires recipients' self-certifications,[10] and triennial reviews that its regional offices conduct.

In April 2021, FTA issued to the regional offices its approach[11] to oversight of the nearly $70 billion in funding the Agency will expend in grants to support the transit industry's COVID-19 response and recovery efforts. The Agency is currently obligating its $25 billion in CARES Act funding to urban and rural programs that receive formula grants. As of July 2021, FTA had awarded 838 grants totaling $24.3 billion and has 89 applications in process requesting approximately $281 million. The act allows for FTA to allocate these funds at up to 100 percent Federal shares with no required local matches.

FTA uses the following financial management systems to approve, process, and disperse COVID-19-related funding.

- The Financial Management System (FMS) is a major mission-critical system that directly supports FTA's financial requirements for processing

[10] FTA relies on each recipient's self-certification that its procurement systems meet FTA requirements and that it has the technical capacity to comply with Federal procurement requirements. Recipients must self-certify as part of the Annual Certification/Assurance Process, which covers a wide range of requirements such as procurement and required by Title 49, U.S. Code, chapter 53.

[11] FTA, *COVID-19 Supplemental Oversight for Federal funding FTA is providing to support the transit industry's COVID-19 response and recovery efforts*, April 2021.

obligations and disbursements of Federal funds to recipients and serves as a data repository for financial information. FMS is also used as a funds control mechanism for processing batch files to and from the Department's financial management system—Delphi, to and from TrAMS, and to and from the ECHO-Web system.[12]

- The Electronic Clearing House Operation Web version 2.0 (ECHO-WEB) is a web application that allows FTA recipients to request payments from their grant awards. It interacts with FMS to ensure that only obligated funds are distributed.
- The Transit Award Management System (TrAMS), is a major application deployed in February 2016, as an efficient, user-friendly, and flexible tool for awarding and managing grants and cooperative agreements and to strengthen the integrity and consistency of FTA's award and management financial and programmatic information.
- The Appian Development Cloud's platform-as-a-service (PaaS) is a hosting and development platform for TrAMS and other applications that enables FTA to manage transit grants and oversee recipient's use of the funds. FTA refers to this platform service as the TrIAD platform.

These systems are interconnected and provide information to Delphi (see figure 1).

[12] FMS is the interface for financial transactions between TrAMS, Delphi, and ECHO-Web, where award information is transmitted nightly.

[redacted]

Two of FTA's systems, TrAMS, and ECHO-Web, are public-facing and together contain information on over 4,900 external users. These users represent over 1,600 local, county, and State transit agencies that receive FTA grant funding.

Since March 2020, the number of cyberattacks on Federal Government information systems has increased through a variety of techniques, including social engineering[13] and phishing.[14] In March 2021, the Government Accountability Office (GAO) issued a report[15] that highlights the lack of progress made on four major cybersecurity challenges—the establishment of a comprehensive cybersecurity strategy and effective oversight; security of Federal systems and information; protection of cyber critical infrastructure;[16] and protection of privacy and sensitive data.

[13] An attempt to trick an individual into revealing information, such as a password, that can be used to attack systems or networks.

[14] An attempt to trick an individual through electronic communication into disclosing sensitive personal information by claiming to be a trustworthy entity.

[15] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO-21-288), March 24, 2021.

[16] Many Federal agencies are responsible for the protection of the Nation's critical infrastructures—such as energy, transportation systems, communications, and financial services. These critical infrastructures are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and wellbeing.

DOT's Cybersecurity Compendium[17] requires the Department's Operating Administrations (OA) and contractors to implement the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF)[18] to establish a process for managing security and privacy risk in the OAs' information systems. FTA's security officials are required to implement the RMF for its financial management systems to help secure the Agency's information systems—computers and networks—and strengthen the risk management process.

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

[redacted]

FTA Does Not Always Properly Select, Document, Implement, or Monitor the Security Controls for Its Financial Management Systems

FTA has not always selected, properly documented and implemented, monitored, or verified the status of some security controls designed to protect the confidentiality, integrity, and availability of its financial management systems.

[17] DOT, *Cybersecurity Compendium*, Supplement to DOT Order 1351.37, version 4.2, March 2018.

[18] NIST Special Publication (SP) 800-37, revision 2, *Risk Management Framework for Information Systems and Organizations*, December 2018.

NIST[19]requires agencies to conduct annual assessments of security controls to determine whether the controls selected are implemented correctly, operating as intended, and producing the desired outcomes concerning meeting the security and privacy requirements for its systems and organization.

However, we found that FTA security officials:

- Did not select and test a required security control for FMS known as process isolation. Process isolation maintains separation between the system's domains—programs and applications—and helps limit the access of possibly untrusted software to other system resources in a secure manner. When system domains are separate, even if someone gets access to the files, domains remain safe. For example, the Agency has not set up different hardware and software technologies for FMS to protect the systems' processes on the operating system. This control also protects the integrity of the hardware and software that performs security function isolation for information systems. FTA security officials stated that the Agency selects security controls according to the departmental policy[20] which is based on the NIST baseline for moderate systems; they stated further that this control was not part of DOT's minimum baseline as required by NIST. FTA is in the process of updating all SSPs to address this required security control.
- Did not properly assess security controls for FMS, ECHO-Web, and TrAMS to ensure that the systems were operating as intended and producing the desired outcomes. FTA security officials mislabeled and incorrectly documented over 180 security controls in the fiscal year 2020 SSPs for these systems and platform. Specifically, FTA security officials mislabeled over 70 security controls for FMS, over 60 for ECHO-Web, and over 50 for TrAMS with the incorrect control type—system-specific or common control. This mislabeling raised a question about whether the individual responsible for testing each system's controls was the system owner or common control provider. Furthermore, FTA security officials provided the Agency's independent assessor[21] the incorrect SSP for its fiscal year 2020 security control assessments for each financial management system

[19] NIST SP 800-37 revision 2, *Risk Management Framework for Information Systems and Organizations*, December 2018.

[20] DOT's Cybersecurity Compendium Supplement to DOT Order 1351.37 version 4.2, March 2018.

[21] A security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the controls' overall effectiveness—the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome.

despite NIST guidance.[22] NIST guidance states that before security control assessments, agencies should select the controls for each system, provide a methodology for how to implement and assess the controls, and document them in the SSP. However, FTA security officials provided the fiscal year 2019 SSP instead of the fiscal year 2020 SSP for review and assessment, stating that the fiscal year 2020 SSP was not available.

- Did not effectively monitor the security risks associated with its financial management systems' inherited controls.[23] FTA security officials did not monitor and verify whether the security controls it inherited from DOT's common control provider were tested, creating a significant risk of compromise. For example, in fiscal year 2020, FTA security officials did not receive test results for the following controls that the Agency had inherited from DOT's common control provider, IT Shared Services Common Operating Environment (ITSS-COE):

    1. 74 of 118 controls inherited for FMS;
    2. 55 of 117 controls inherited for ECHO-Web; and
    3. 10 of 34 controls inherited for TrAMS.

[redacted]

[redacted]

Because FTA did not always effectively select, document, implement, and monitor all security controls for its financial management systems, authorizing officials may not have accurate pictures of security risks. As a result, the authorizing

[22] NIST SP 800-37 revision 2, *Risk Management Framework for Information Systems and Organizations*, December 2018.

[23] A control is deemed inherited when the system or program receives protection from the implemented control, but the control is developed, implemented, assessed, authorized, and monitored by an internal or external entity other than the entity responsible for the system or program.

officials may not be able to accurately determine whether security controls are implemented correctly, operating as intended, and producing the desired outcomes to satisfy security requirements.

FTA Has Not Remediated Longstanding Security Control Weaknesses for Its Financial Management Systems

FTA has not remediated weaknesses in the security controls for its financial management systems since 2016. These weaknesses include issues with multifactor user authentication (MFA), outdated databases, integrity tools, and contingency planning and incident response.

According to NIST[24] guidelines, breach of a system categorized as moderate—as FTA's financial management systems are categorized—could expose the organization to significant financial loss, erosion of customer confidence, and damage to its operations. FTA officials stated that controls for which a POA&M exists are reviewed yearly for risk and quarterly for remediation discussions. If a POA&M cannot be remediated within the year, it is reevaluated at the beginning of the next assessment to determine continued risk-acceptance.

[redacted]

[redacted]

The Office of Management and Budget (OMB) calls[25] for agencies to require [redacted] FTA security officials informed us that they have accepted this risk and indicated that

[24] NIST, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004.

[25] OMB Memorandum 19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management,* May 2019.

[redacted]

[redacted]

[redacted] TrAMS and ECHO-Web were evaluated and accepted until the Agency can implement a viable solution. [redacted]

Cybersecurity attacks are one of the biggest security threats present today. In 2017, OMB provided guidance[30] to Federal agencies on when grant recipients should report breaches to their awarding agencies. We found that between May and August 2020, three FTA recipients were victims of cyber-attacks that exposed personally identifiable information (PII),[31] personnel data, and financial data.

- Texas Department of Transportation (TXDOT) officials stated that in May 2020, the Agency experienced a ransomware attack[32] that left several

[26] User role-based access is a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role. A role permission may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization.

[27] Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, 79 Fed. Reg. 63489, October 23, 2014.

[28] These implementation steps are set forth in OMB Circular A-130, Appendix I.

[29] NIST SP 800-63-3, *Digital Identity Guidelines*, June 2017.

[30] OMB Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017.

[31] Information on individuals such as names, social security numbers, addresses, salaries, benefits, and banking information.

[32] Ransomware encrypts files and demands a "ransom" payment before the attacker unencrypts the files.

parts of its information network unavailable. To prevent further unauthorized access, TXDOT officials isolated the affected network areas.

- In July 2020, Trinity Metro, the regional transit agency in Fort Worth, TX, experienced a "double extortion”[33] attack. A ransomware cyberattack compromised Trinity's phone lines, its booking system, employees’ PII, and vendor financial documentation. The attack left Trinity with limited communication.
- In August 2020, staff at the Southeastern Pennsylvania Transportation Authority (SEPTA)—the transit agency that serves the greater Philadelphia area—discovered suspicious activity that indicated unauthorized access to some of its servers. The attack may have exposed the PII of over 9,300 SEPTA employees.

In 2021, two more FTA recipients were victims of cyber-attacks.

- In April 2021, hackers claimed to have stolen data from the Santa Clara Valley Transportation Authority (VTA) in a ransomware attack that paralyzed many of the Agency’s computer systems. VTA shut down its computer network to contain the event.
- In June 2021, New York City's Metropolitan Transportation Authority (MTA) publicly announced that in April 2021, cyber attackers had breached at least one of its virtual private networks, allowing access to at least 3 of the Agency’s 18 databases. The cyberattack did not compromise customer or employee PII but prompted officials to notify 3,700 MTA employees and contractors to change their passwords—an indication that MTA lacks MFA mechanisms in its computer network.

According to a surface transit cyber preparedness report by San Jose State University’s Mineta Transportation Institute,[34] given the multitude of connected devices that the transit industry uses and the vast amount of data the industry generates, the transit industry is vulnerable to cyberattacks such as ransomware. The report also indicates that attackers frequently implement ransomware through email which is the most common path for phishing attacks.

On May 12, 2021, the President issued an Executive order[35] that requires Federal civilian agencies to adopt within 180 days MFA requirements for users and

[33] A ransomware attack combined with data leak extortion. The ransomware encrypts files and demands payment; the data leak extortion steals data prior to encryption and demand for ransom payment.

[34] Mineta Transportation Institute, *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, September 2020.

[35] Executive Order 14028, *Improving the Nation’s Cybersecurity*, May 12, 2021.

encryption for data at rest and in transit to the maximum extent consistent with Federal law. If an agency chooses not to adopt these measures, the agency head must provide a written rationale to the Secretary of Homeland Security, Director of the Cybersecurity and Infrastructure Security Agency, Director of OMB, and the President's National Security Advisor. [redacted]

[redacted]

[redacted]

To properly implement configuration settings, DOT's Cybersecurity Compendium requires OA security officials, such as systems owners, to

- ensure that only approved configuration settings are used for products deployed in the information system, and document implementation responsibility by the information system owner;
- ensure that all endpoints, web applications, databases, and custom-developed software packages are deployed in compliance with the established configuration and patching baseline approved by OCIO; and
- identify and document any settings that deviate from approved settings and obtain approval for the deviations from DOT's Chief Information Security Officer.

[redacted]

[36] A set of parameters, which can be changed as needed, in hardware, software, or firmware that affects the security posture and/or functionality of an information system.

[redacted] also inhibits the preventive maintenance necessary to keep an information system stable and safe from malicious software and other threats that could result in unauthorized system access.

[redacted]

[redacted]

FTA officials acknowledged these system deficiencies as security weaknesses and agreed to meet with departmental security officials to address them. [redacted] risk that unauthorized access could compromise the systems' financial records and user data.

FTA Lacks Effective Contingency Planning and Incident Response Capabilities for Its Financial Management Systems

FTA has not implemented an alternate set of personnel to restore its financial management systems if its primary personnel are unavailable. Per the Department's Cybersecurity Compendium, OAs' system owners must ensure that primary and alternate resources are assigned for each contingency-related role. Additionally, contingency planning addresses both information system restoration and implementation of alternative mission and business processes when systems are compromised. Each OA must test its contingency planning activity on an annual basis.

[redacted] [redacted]

We found that FTA has not implemented the use of alternate contingency personnel for FMS and Echo-Web since 2016. FTA officials informed us that additional personnel to serve as a backup for each contingency planning role would require it to incur unnecessary costs. However, this lack of alternate contingency personnel could impact FTA's ability to properly respond to a system disruption such as a hardware failure or a cyberattack and could result in a single point of failure if primary personnel become unavailable.

Furthermore, FTA has not verified that its incident and data response plan (IDRP) would be reliable if either FTA or its common control provider experiences a security incident or data breach. Agency security officials did not provide evidence that they have documented the performance of incident response scenarios for FMS and ECHO-Web in accordance with NIST guidance.[38] FTA indicated that as a part of its continuous monitoring, it is planning to perform separate incident response testing outside of contingency plan testing. NIST guidance states that an organization's incident response team should plan its incident coordination with external parties before an incident occurs to ensure that all parties know their roles and that effective lines of communication are established. However, FTA officials stated that the Agency has not developed separate test scenarios for its IDRP because the scenarios are included in the Agency's disaster recovery testing to minimize the unnecessary impact on resources. Incident response is a responsibility shared by FTA and ITSS-COE. However, ITSS-COE's security incident event management tool does not meet standards, properly identify suspicious activities, or quickly correlate data.

Finally, we found a major security risk in FTA's lack of oversight and reporting of its recipients' security incidents.

- FTA was not aware of four of the five recipients' cybersecurity attacks between May 2020 and April 2021 and did not report on the other incident to the Department's security operations center (SOC).
- FTA also does not currently require its recipients to report breaches of PII or security incidents despite OMB and departmental requirements to do so. OMB states[39] that when recipients use Federal information systems that contain PII, awarding agencies must ensure that recipients have procedures to respond to a breach and notify their awarding agency of the breach. Similarly, DOT's incident response plan,[40] which applies to all DOT employees, contract personnel, and others who have authorized

[38] NIST SP 800-53, rev 4; NIST SP 800-61, rev. 2.

[39] OMB Memorandum M-17-12, January 2017.

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

access to DOT information systems, requires recipients to report security incidents that impact networks' and systems' security.

- FTA did not take appropriate action when a recipient reported a security incident to regional administrator. FTA's Information Systems Security Manager/Privacy Officer did not report the recipient's incident to DOT's SOC once the regional administrator learned of the incident.

FTA security officials also do not have a mechanism in place to ensure that recipients report security incidents as required by DOT policy.[41]

This lack of tracking and documenting recipients' security incidents may result in the compromise of usernames and credentials and expose FTA to cyberattacks that may delay the distribution of COVID-19 related funds to recipients.

[redacted]

[redacted]

The Department of Homeland Security (DHS) defines TIC use requirements in what it calls Use Cases. In TIC Use Cases, DHS outlines alternative security controls such as endpoint and user-based protections that must be in place if an agency does not direct its network traffic through a TIC. DHS policy[43] allows agencies to implement Use Cases if necessary based on security architecture.

Due to performance issues caused by the increase in traffic on public infrastructure during the COVID-19 pandemic, FTA received temporary DOT approval to [redacted]

[41] DOT's Cybersecurity Incident Response Plan.

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

[43] DHS, *Cybersecurity and Infrastructure Security Agency Use Case Handbook*, 2021; *Cybersecurity & Infrastructure Security TIC 3.0 Core Guidance Documents*, retrieved from https://www.cisa.gov/publication/tic-30-core-guidance-documents .

[redacted]

[redacted]

Conclusion

Security controls for FTA financial management systems protect the systems and help protect the Federal dollars recorded in those systems. These controls must be appropriately identified, tested, implemented, and monitored to operate effectively. However, FTA's security officials cannot determine whether the security controls are implemented correctly, operating as intended, and producing the desired outcomes on security requirements. Additionally, FTA has not addressed longstanding security weaknesses such as the lack of MFA and outdated databases used since 2016. Furthermore, FTA has reviewed and accepted the risks for identified security control weaknesses in its financial management systems and acknowledged some risks may not be possible to remediate due to application limitations, absence of available tools, or guidance from DOT. Until FTA strengthens its security controls and remediates cybersecurity weaknesses, the Agency will not have a true picture of the risks to its financial management systems or know whether the billions of dollars in COVID-19 funding these systems support are susceptible to significant financial loss.

Recommendations

To remediate long-standing computer security weaknesses and improve FTA's cybersecurity posture for its financial management systems, we recommend that the Federal Transit Administrator:

1. Select and implement security control-process isolation to protect its financial management systems (FMS and ECHO-Web) against risk.

2. Perform an assessment of its financial management systems (FMS, ECHO-Web, and TrAMS) security controls that at a minimum reflect the correct

security control types and update each system's system security plan with the correct control types.

3. Update the security assessment documents for its financial management systems (FMS, ECHO-Web, and TrAMS) to properly reflect the results of all security controls (e.g., common, hybrid, and system-specific) for selection, implementation, and assessment, per DOT requirements.

4. Obtain and assess all up-to-date security authorization documents associated with its financial management systems (FMS, ECHO-Web, and TrAMS) inherited controls (e.g. common, hybrid) to determine and monitor the effectiveness of its inherited controls and risk per NIST & DOT security requirements.

5. [redacted]

6. [redacted]

7. Implement secure configuration settings for its financial management systems (FMS and ECHO-Web) databases in accordance with Federal and DOT policies.

8. [redacted]

9. Develop and implement a plan that ensures continuity of federal workforce and contractual resources to fulfill contingency responsibilities for its financial management systems (FMS and ECHO-Web) to maintain continued operations should an emergency event incapacitate the primary personnel.

10. Conduct, document, and communicate the results of its annual incident response and data breach plan testing for financial management systems before authorization to operate; to ensure effectiveness in the event of a security incident or data breach is discovered within FTA or an external party (e.g. FTA recipient, common control provider).

11. Establish, document, and implement a security incident reporting process and procedures for its recipients to report incidents that affect their login credentials.

12. Require the FTA Information System Security Manager (ISSM)/ Privacy Officer to adhere to its Incident and Data Breach Response Plan to report

recipient cybersecurity incidents involving FTA information systems or user accounts.

[redacted]

Agency Comments and OIG Response

We provided FTA with our draft report on August 23, 2021, and received its formal response on September 22, 2021. FTA's response is included in its entirety as an appendix to this report. FTA concurred with all of our 13 recommendations and provided appropriate actions and completion dates for recommendations 5 through 13.

FTA has informed us that it has implemented recommendations 1 through 4. On September 1, 2021, FTA provided supporting documentation for our review and requested that we close the recommendations within 30 days after issuing the final report.

Actions Required

We consider recommendations 1 through 4 resolved but open pending our evaluation of documentation FTA has provided. We will provide our response to FTA within 30 days after issuing our final report. We consider the recommendations 5 through 13 resolved but open pending completion of the planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between November 2020 and August 2021 in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This is a self-initiated audit and as part of our methodology, we assessed the effectiveness of FTA's financial management systems' security controls designed to protect the confidentiality, integrity, and availability of the systems and their information. We also

- gained an understanding of the security controls, and other internal controls FTA has in place for managing the information systems that process, store, or transmit Coronavirus Aid, Relief, and Economic Security (CARES) ACT funding information;
- obtained documentation and evaluated it against Federal information security laws, regulations, and department-wide policies and procedures; we also obtained and evaluated all contract documentation, other formal agreements to ensure appropriate IT security language and/or clauses are present;
- attended a high-level overview of FTA's financial management systems to gain an understanding of FTA's grant funding process;
- interviewed departmental security operations center personnel to obtain information on security incident reporting;
- interviewed FTA program and security officials as well as contractor support personnel;
- analyzed each FTA financial management information systems' security authorization documentation to determine whether FTA selected, assessed, implemented, and monitored security controls per policy;
- reviewed previously reported security control deficiencies for FTA's financial management systems and assessed the effectiveness of corrective actions taken to address them;

- reviewed and validated user account information for FTA's financial management systems; and
- analyzed information on security incidents and verify whether FTA has process and procedure in place to address them.

We conducted our audit work remotely due to mandatory COVID-19 telework at DOT Headquarters in Washington, D.C. Furthermore, we conducted virtual meetings with FTA and departmental officials along with third-party contractors as required.

Exhibit B. Organizations Visited or Contacted

FTA Headquarters Facilities

Office of Information Technology

Office of Financial Systems

Office of Budget and Policy

Office of Strategic Planning and Analysis

Office of Administration

Office of Chief Counsel

Other Organizations

Office of the Secretary, Audit Relations and Program Improvement

Office of the Secretary, Chief Information Officer

Department of Transportation, Office of General Counsel

General Services Administration, Federal Risk and Authorization Management Program (FedRAMP) Program Management Office

Federal Aviation Administration, Office of Finance and Management, Office of Information & Technology Services

Federal Aviation Administration, Office of National Security Programs & Incident Response

Exhibit C. List of Acronyms

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
COE	Common Operating Environment
DOT	Department of Transportation
Echo-Web	Electronic Clearing House Operation Web Version 2.0
EO	Executive order
FMS	Financial Management System
FTA	Federal Transit Administration
GAO	Government Accountability Office
ITSS	IT Shared Services
MFA	Multi-factor Authentication
MTA	Metropolitan Transportation Authority
NIST	National Institute of Standards and Technology
OA	Operating Administration
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RMF	Risk Management Framework
SP	Special Publication
SSP	System Security Plan
TIC	Trusted Internet Connection
TrAMS	Transit Award Management System
TriAD	Transit Integrated Appian Development
TXDot	Texas DOT

Exhibit D. Major Contributors to This Report

NATHAN CUSTER	PROGRAM DIRECTOR
STACY JORDAN	PROJECT MANAGER
MARTHA MORROBEL	SENIOR IT SPECIALIST
JO'SHENA JAMISON	SENIOR IT SPECIALIST
NELSON FLORES	IT SPECIALIST
SUSAN NEILL	WRITER-EDITOR
TOM DENOMME	CONSULTANT
CELESTE BORJAS	ASSOCIATE COUNSEL

Appendix. Agency Comments

Memorandum

U.S. Department
of Transportation
**Federal Transit
Administration**

Subject:	INFORMATION: Management Response – Office of Inspector General (OIG) Draft Report – FTA's Security Controls for Financial Management Systems	Date:	SEP 2 2 2021
From:	Nuria Fernandez Administrator Federal Transit Administration	Reply to Attn. of:	Chris Paul (202) 366-6076
To:	Kevin Dorsey Assistant Inspector General for Information Technology Audits		

FTA is committed to safeguarding COVID-19 funds, including the Coronavirus Aid, Relief, and Economic Security Act, Coronavirus Response and Relief Supplemental Appropriations Act, and American Rescue Plan Act funds through its financial management systems. FTA has processed over $38 billion in COVID-19 funding with no major incidents involving the Electronic Clearing House Operation (ECHO), the Financial Management System (FMS), or the Transit Award Management System (TrAMS). These systems undergo regular internal reviews and audits to ensure compliance with requirements and to improve security.

To further bolster our IT security, FTA is taking the following actions to carry out timely solutions to ensure our financial systems have sound internal controls:

- [redacted]

[redacted]

[redacted]

[redacted]. FTA has implemented recommendations 1 - 4 and on September 1, 2021, provided supporting documentation to the OIG and requested that the OIG close the recommendations within 30 days after issuing the final audit report. For recommendations 5 - 6 and 8 - 12, FTA will complete planned actions by December 31, 2021. For recommendations 7 and 13, FTA will complete actions by December 31, 2022.

We appreciate the opportunity to comment on OIG' s draft report. Please contact Chris Paul, FTA's Audit Liaison Program Manager, at (202) 366-6076 with any questions.

Sincerely,

Nuria I. Fernandez

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety ☎ Hotline

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

OUR MISSION

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

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