AMTRAK

OFFICE *of* INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

INFORMATION TECHNOLOGY:

Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity

OIG-A-2023-002 | November 7, 2022

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

This page intentionally left blank.

~~SENSITIVE SECURITY INFORMATION~~

AMTRAK OFFICE of INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

Memorandum

To: Christian Zacariassen
Executive Vice President/Digital Technology and Innovation

Laura Mason
Executive Vice President/Capital Delivery

Gerhard Williams
Executive Vice President/Service Delivery and Operations

From: Jim Morrison
Assistant Inspector General, Audits

Date: November 7, 2022

Subject: *Information Technology: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity* (OIG-A-2023-002)

Cyber-related breaches of operational technology (OT) systems[1]—which manage the nation's critical infrastructure—are increasing. For example, in 2021, a cybersecurity breach shut down the operations of one of the largest refined petroleum pipelines in the United States. OT systems typically were once closed environments—that is, they were not connected to external technology networks. In recent years, however, many organizations, including Amtrak (the company), have increasingly integrated their OT systems with the information technology systems their employees and customers use, putting them at greater risk of cybersecurity threats.

[1] OT systems monitor and control physical processes or interact with the physical environment, as opposed to information technology, which are primarily used for computing data. OT systems include physical assets (known as "hardware"), such as servers and desktops, and non-physical assets (known as "software"), such as applications, operating systems, and databases. Collectively, these technology assets are components of OT systems.

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

Four types of OT systems support the company's train operations: (1) Dispatching, (2) Communications and Signals, (3) Electric Traction, and (4) Positive Train Control (PTC). If compromised, these systems could pose a serious safety and operational risk, as the company relies on them to dispatch trains, monitor and control train movements, manage the flow of electricity to locomotives, and control train signals and other communications equipment.

Accordingly, our objective was to assess the effectiveness of the company's practices for identifying and tracking its OT assets to facilitate its ability to protect them from cybersecurity threats. To achieve our objective, we interviewed company officials in the Digital Technology and Innovation, Capital Delivery, and Service Delivery and Operations departments to determine if roles and responsibilities were clear to ensure effective identification and tracking of OT assets for cybersecurity purposes. We also reviewed company policies and procedures to determine if they include inventory processes and follow industry standards. In addition, we reviewed company inventories of OT assets. Lastly, we identified challenges that limit the company's ability to protect its OT assets. For more information on our scope and methodology, see Appendix A.

SUMMARY OF RESULTS

The company does not effectively identify and track its OT assets for cybersecurity purposes. Contrary to industry standards, the company's Information Security group, which is responsible for the company's cybersecurity program, does not have complete inventory data on all OT assets to identify and mitigate cyber risks. As a result, Information Security is not able to effectively address the security vulnerabilities of these assets, [redacted]—increasing the risk of cyberattacks that could disrupt mission-critical operations.

The company's practices for identifying and tracking OT assets are not effective because it does not manage the cybersecurity of these assets with an enterprise-wide approach. Accordingly, we identified five factors that would improve the governance of OT assets

[redacted]

To improve the effectiveness of company practices and enterprise-wide cybersecurity governance for OT assets, we recommend the company establish a governing body—such as a cross-departmental working group—to facilitate its efforts to identify and track OT assets. Leveraging the working group's collective knowledge, we also recommend the company decide and plan for the OT asset management system it will use for its cybersecurity needs, implement policies and procedures with clear roles and responsibilities, and develop complete network maps. In commenting on a draft of this report, company executives agreed with our recommendations and described actions the company took or plans to take by December 2023 to address them. For management's complete response, see Appendix B.

BACKGROUND

The company's OT systems include assets it manages as well as assets third-party vendors manage and support on its behalf. The company uses four key types of OT systems called "train control" systems:

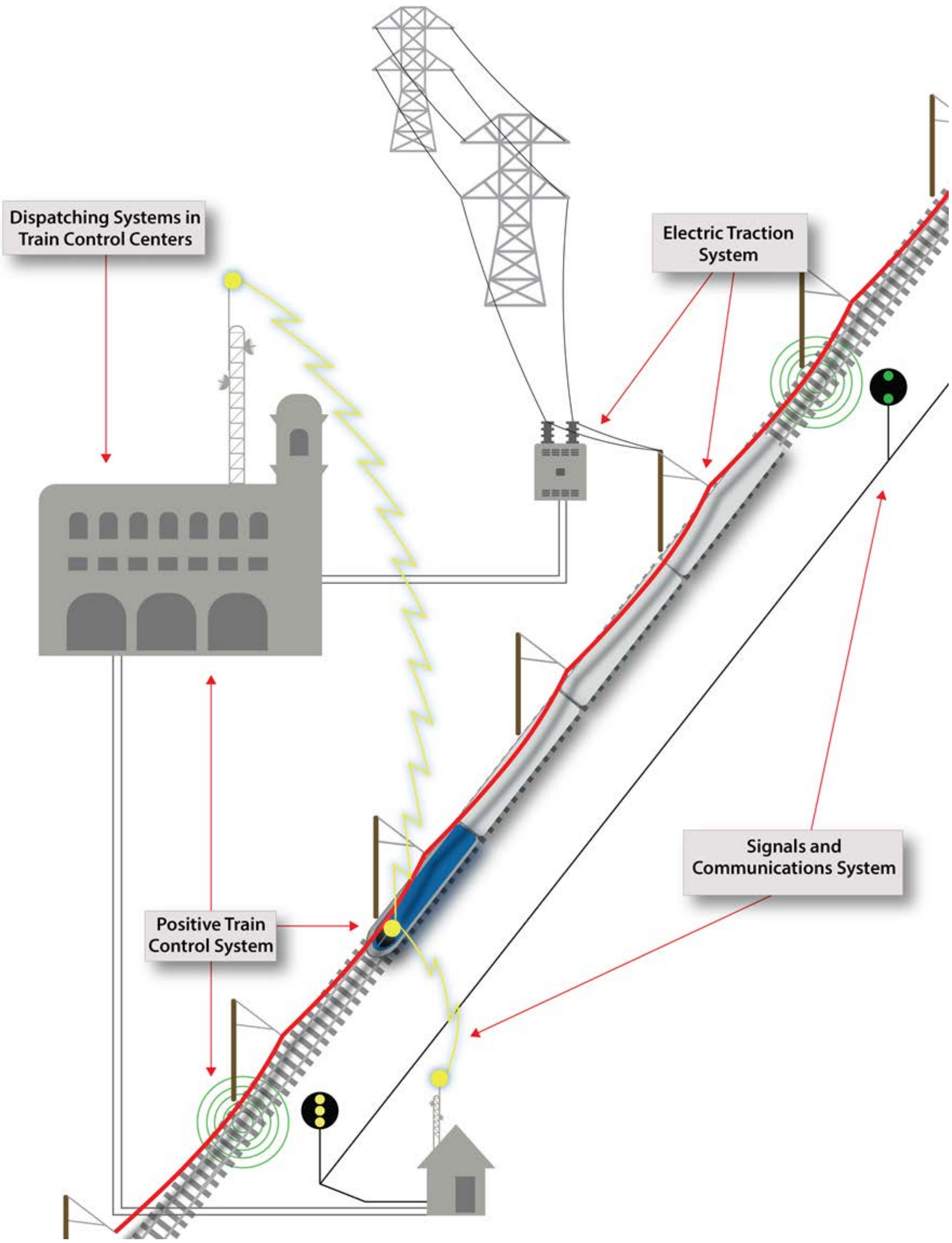
- **Dispatching** systems allow train control center personnel to dispatch and monitor trains.

- **Communications and Signals** systems allow train dispatchers to remotely control signal indicators and interlockings[2] and to communicate with train crews and other information technology systems via radio and data transmissions.
- **Electric Traction** systems control the flow of electricity from suppliers to overhead catenary and electric trains through substations.
- **PTC** systems monitor and control train movements and automatically slow or stop a train to help prevent accidents. The company has identified PTC as its key safety system for preventing train collisions.

Figure 1 provides an illustration of these OT systems as the company uses them on the Northeast Corridor.

[2] An interlocking is a system of signals and switches that are used to control train traffic—for example, at a crossing of two railroads.

Figure 1. Key Operational Technology Systems Used on the Northeast Corridor


Dispatching Systems in Train Control Centers
Electric Traction System
Signals and Communications System
Positive Train Control System

Source: OIG analysis of PTC design documents

Three company departments oversee the technology assets used within the four OT systems:

- The **Digital Technology and Innovation department**, led by the Executive Vice President/Digital Technology and Innovation, includes the Chief Information Security Officer, who is responsible for the company's cybersecurity program. The department is also responsible for identifying and tracking technology assets within the Dispatching system. In addition, it is responsible for coordinating with third-party vendors providing back-office support for the Electric Traction system and the company's three PTC systems.[3]

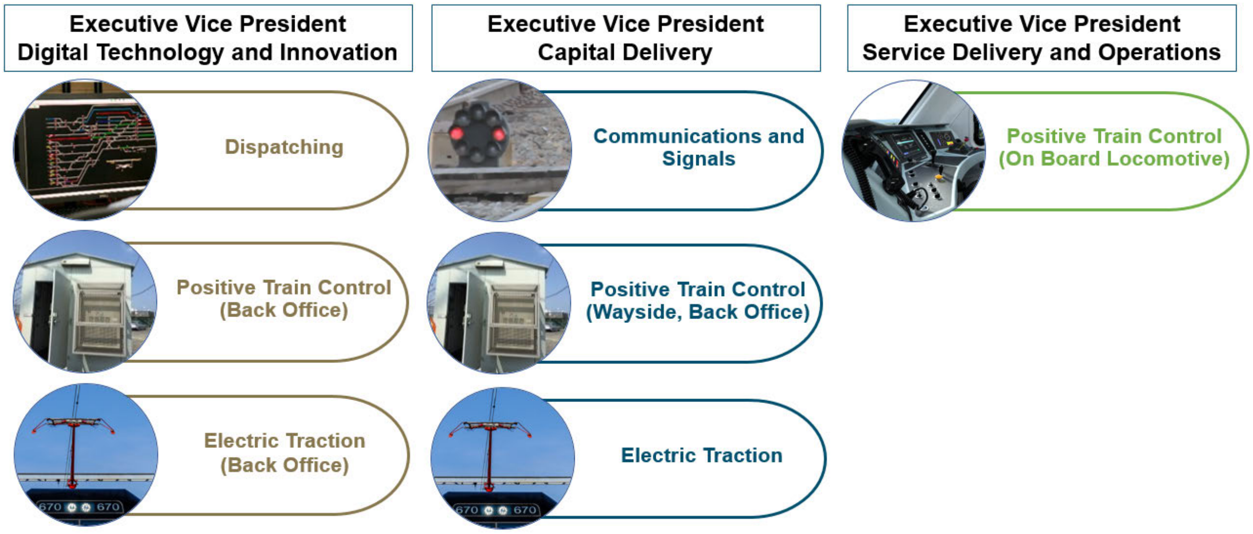
- The **Capital Delivery department,** led by the Executive Vice President/Capital Delivery, is responsible for identifying and tracking assets within the Communications and Signals system. These include communication networks and technology assets along railroad tracks—wayside and at the train stations. The department is also responsible for technology assets for the Electric Traction system and PTC systems.

- The **Service Delivery and Operations department**, led by the Executive Vice President/Service Delivery and Operations, is responsible for identifying and tracking PTC-related technology assets on individual locomotives.

Figure 2 shows the three company departments that oversee the company's four OT systems.

[3] The company has implemented three types of PTC systems: Interoperable Electronic Train Management System, Advanced Civil Speed Enforcement System, and Incremental Train Control System.

Figure 2. Departments Responsible for Operational Technology Systems


Executive Vice President
Digital Technology and Innovation
Dispatching
Positive Train Control (Back Office)
Electric Traction (Back Office)
Executive Vice President
Capital Delivery
Communications and Signals
Positive Train Control (Wayside, Back Office)
Electric Traction
Executive Vice President
Service Delivery and Operations
Positive Train Control (On Board Locomotive)

Source: OIG analysis of information that company employees provided, March through August 2022

The company recently adopted guidelines set forth by the National Institute of Standards and Technology (NIST), which publishes leading industry standards for cybersecurity. NIST suggests organizations use a layered security approach with multiple levels of defense to protect their OT systems from cybersecurity threats. One of the first steps is for organizations to develop a complete inventory of OT assets that accurately reflects their systems.[4] According to NIST guidance, an inventory should include detailed data on OT assets such as how critical they are to operations, as well as more specific information like an asset's Internet Protocol address, version number, model number, physical location, date of installation, and manufacturer. These detailed data enable organizations to prioritize their most critical assets and identify controls to secure and protect them from unauthorized access. NIST also suggests organizations maintain a centralized asset management system for their OT inventory.

[4] NIST, *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53, Revision 5*, September 2020; NIST, *Guide to Industrial Control Systems Security, Special Publication 800-82, Revision 2*, May 2015; and NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018.

Further, the November 2021 passage of the Infrastructure Investment and Jobs Act provided the company access to as much as $66 billion in funding.[5] Projects eligible for funding under this act include those that aim to eliminate the backlog of the company's obsolete technology assets, such as systems for reservations, security, training centers, and other information technology.

INCOMPLETE INVENTORY DATA ON OPERATIONAL TECHNOLOGY ASSETS LIMIT CYBERSECURITY OVERSIGHT

The company's practices for identifying and tracking its OT assets are not effective in facilitating its ability to protect them from cybersecurity threats. Specifically, the company's management of its OT assets is siloed—the operational departments that use the company's OT assets each maintain a piece of the company's asset inventory, but the departments store these pieces in unconnected systems and spreadsheets, as Figure 3 shows.

Figure 3. Inventory Locations of Operational Technology Assets

Dispatching | Communications and Signals | Electric Traction | Positive Train Control

[redacted]

Source: OIG analysis of information that company employees provided, March through August 2022

[5] Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021).

These operational silos limit Information Security's ability to easily access and review complete inventory data on all OT assets needed to identify and mitigate cyber risks. Further, Information Security officials told us that these inventories often did not have the details necessary to protect the assets from cyber threats that NIST standards suggest having, such as serial and model numbers. For example, when manufacturers identify security updates to protect assets from known vulnerabilities, Information Security staff can use these asset details—serial and model numbers—to quickly identify all affected assets and install the updates. Without complete inventory data, the company faces the following challenges that limit its ability to effectively protect its OT assets, increasing the risk of cyberattacks that could disrupt mission-critical operations.

Security Vulnerabilities

Information Security does not have the inventory data necessary to determine whether outdated assets or those with known security vulnerabilities are on the company's OT network.[6] For example:

- Information Security received a security alert from the Department of Homeland Security[7] concerning a particular vulnerability that a hacker could exploit. Information Security could not, however, quickly identify the potentially impacted assets on the company's OT network. Instead, it had to email five business department employees to determine whether they knew of any assets that this vulnerability could affect. Relying on the departments' business staff instead of having immediate access to complete inventory data that accurately reflects the company's OT systems impedes Information Security's ability to react [redacted] increases the risk of successful cyberattacks.

[6] An OT network is a group of systems that are connected and communicate with one another for a common purpose, such as moving trains.

[7] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency connects industry and government to each other and to resources, analyses, and tools to help them build their own cyber resilience.

- One vendor did not remove an outdated OT asset—that is, one that the vendor and manufacturer no longer supported—from its network. During a routine scan, Information Security discovered that this asset tried to connect to a server in Iran. Although Information Security disconnected it from the network without any adverse effects, having complete inventory data would have helped the company identify and remove this outdated asset before the incident occurred.

- Until we alerted Information Security, it was unaware of one outdated asset on the company's OT network that the manufacturer had not supported for more than ten years. The manufacturer's website identified seven known security vulnerabilities with this asset, including the possibility of a remote attacker controlling user access. [redacted] told us that they do not plan to replace this vulnerable asset and disconnect it from the company's OT network until they replace the other assets it supports, which will take at least two years. An Information Security official told us that the cyber risk for this asset is low because it connects to a restricted portion of the network and only does so when in use, which the asset owners said is infrequent. Nonetheless, complete inventory data would have helped Information Security identify this vulnerability so that it could monitor the asset until it is replaced.

In the absence of complete inventory data, Information Security uses a tool that periodically scans the OT network to identify security vulnerabilities, but the tool is limited in its ability to identify at-risk OT assets the company has. During our review, business department staff told us about three additional examples of outdated assets on the OT network. Information Security, however, was unable to use the tool's network scan results to confirm this. Furthermore, although the tool captures some asset details, it had several missing data fields that Information Security would need. Relying on such tools instead of real-time inventory data delays Information Security from quickly

[redacted]

[redacted]

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

[redacted]

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

[redacted]

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

[redacted]

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

[redacted]

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

[redacted]

[9] A network boundary establishes how data flow through devices or from one network to another.

[10] *Human Resources: The Company is Addressing Engineering Management Workforce Challenges, but Additional Work Remains,* (OIG-A-2022-012), July 12, 2022; and *Human Resources: Department Will Face Challenges Supporting Workforce Growth Plans,* (Interim Audit Report OIG-A-2022-003), December 7, 2021.

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

CONCLUSIONS

[redacted]

RECOMMENDATIONS

To establish an enterprise-wide approach to governing the company's OT assets and better protect them from cybersecurity threats, we recommend the company:

1. Establish a body, such as a cross-departmental working group, to leverage the expertise of Information Security and the business departments managing the four OT systems.

Using the collective knowledge of the working group members, we recommend the company:

2. Decide how, and through what system, Information Security will obtain the complete OT inventory data that it needs and develop a plan with the necessary technical requirements to implement that decision.
3. Develop and implement enterprise-wide policies and procedures—including clear roles and responsibilities for all key stakeholders—as well as training for maintaining complete OT asset inventory data for cybersecurity purposes.
4. Develop complete network diagrams on the company's OT assets.

MANAGEMENT COMMENTS AND OIG ANALYSIS

[redacted]

[11] Management stated that it took these actions when our draft report was with the company for comment. We will review company actions taken during our comment period as part of our standard recommendation follow-up process.

[redacted]

APPENDIX A

Objective, Scope, and Methodology

This report provides the results of our review of the company's efforts to maintain complete inventory data on OT assets for cybersecurity purposes. Our objective was to assess the effectiveness of the company's practices for identifying and tracking its OT assets to facilitate its ability to protect them from cybersecurity threats. Our scope included reviewing the company's practices for identifying and tracking technology assets for four types of systems supporting train operations: (1) Dispatching, (2) Communications and Signals, (3) Electric Traction, and (4) PTC. We defined technology assets as devices with software or hardware that systems use to exchange information on the network. We performed our work from March 2022 through August 2022. Certain information in this report has been redacted due to its sensitive nature.

To perform our work, we interviewed company officials in the Digital Technology and Innovation, Capital Delivery, and Service Delivery and Operations departments to understand their roles and responsibilities in identifying and tracking OT assets and determined the inventory locations for these assets. We also interviewed officials and staff from Information Security to determine if they have complete inventory data and network diagrams on all OT assets to identify and mitigate cyber risks.

We also reviewed company policies and procedures to determine if they include clear roles and responsibilities for OT asset inventory management and whether these policies provided guidance on the type of OT asset data Information Security needs to facilitate its cybersecurity efforts. Additionally, we reviewed company inventories of OT assets to determine whether (1) the company used [redacted] the company's asset management database for identifying and tracking OT assets, and (2) data on the OT assets included specific information NIST suggests such as an asset's Internet Protocol address, version, serial, and model number. Lastly, we identified challenges that limit the company's ability to effectively identify security vulnerabilities, [redacted]

We conducted this performance 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Internal Controls

We reviewed the internal controls the company had in place for identifying and tracking its OT assets for cybersecurity purposes. Specifically, we assessed the internal control components and underlying principles and determined that the following three internal control areas were significant to our audit objective:

- **Control environment.** Management should establish an organizational structure, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- **Control activities.** Management should develop and implement activities through policies and procedures to ensure that the company achieves its objectives.
- **Information and communication.** Management should provide quality information to achieve the entity's objectives.

We developed audit work to ensure that we reviewed each of these internal control areas, including assessing the following:

- program management controls for establishing clear roles and responsibilities for ensuring that enterprise-wide inventory data are complete and accurate from a cybersecurity perspective
- policies and procedures for maintaining an OT asset inventory data for cybersecurity purposes
- the quality and completeness of technology asset data needed by Information Security to assist in protecting the company from cybersecurity threats

Because our review was limited to these internal control components and underlying principles, it may not have disclosed all the internal control deficiencies that may have existed at the time of this audit.

Computer-Processed Data

We obtained computer-processed data from the Service Delivery and Operations department, which we used to analyze whether the company used [redacted] for identifying and tracking OT assets. To verify data reliability, we obtained [redacted] system access and independently performed data validation and verification, including performing basic logic checks, checking for out-of-range data, and other inconsistencies. In addition, we observed company employees maintaining OT asset data in their separate inventories and spreadsheets. We did not obtain these datasets for further analysis, however, given their sensitivity and the needs of our audit. Based on the above steps, we determined that [redacted] data were sufficiently reliable to support our findings, conclusions, and recommendations.

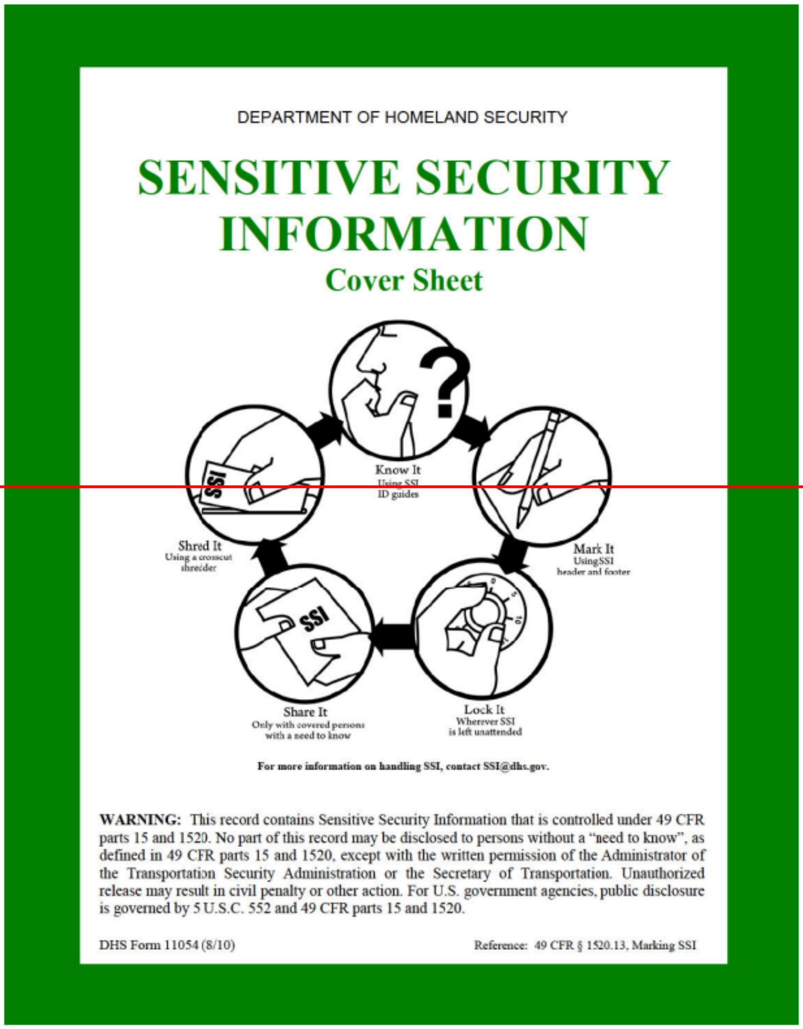
Prior Reports

In conducting our analysis, we reviewed and used information from the following Amtrak OIG reports:

- *Human Resources: The Company is Addressing Engineering Management Workforce Challenges, but Additional Work Remains,* (OIG-A-2022-012), July 12, 2022
- *Information Technology: Better Requirements Could Help the Company Implement Technology Projects More Effectively,* (OIG-A-2022-007), March 11, 2022
- *Human Resources: Department Will Face Challenges Supporting Workforce Growth Plans*, (Interim Audit Report OIG-A-2022-003), December 7, 2021
- *Safety and Security: Amtrak Expects Positive Train Control will be Interoperable with Other Railroads but Could Better Measure System Reliability,* (OIG-A-2021-004), December 11, 2020
- *Information Technology: Mobile Device Security Needs to Improve to Better Protect Company Data from Compromise*, (OIG-A-2020-010), May 8, 2020
- *Information Technology: Improving Cybersecurity and Resiliency of Train Control* Systems Could Reduce Vulnerabilities, (OIG-A-2019-008), July 9, 2019
- *Information Technology: Improving Security of Publicly Accessible Websites Could Help Limit Cyber Risk,* (OIG-A-2018-001), October 23, 2017

APPENDIX B

Management Comments


SSI
Know It
Using SSI
ID guides
Mark It
Using SSI
header and footer
Lock It
Wherever SSI
is left unattended
Share It
Only with covered persons
with a need to know
SSI
Shred It
Using a crosscut
shredder

DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

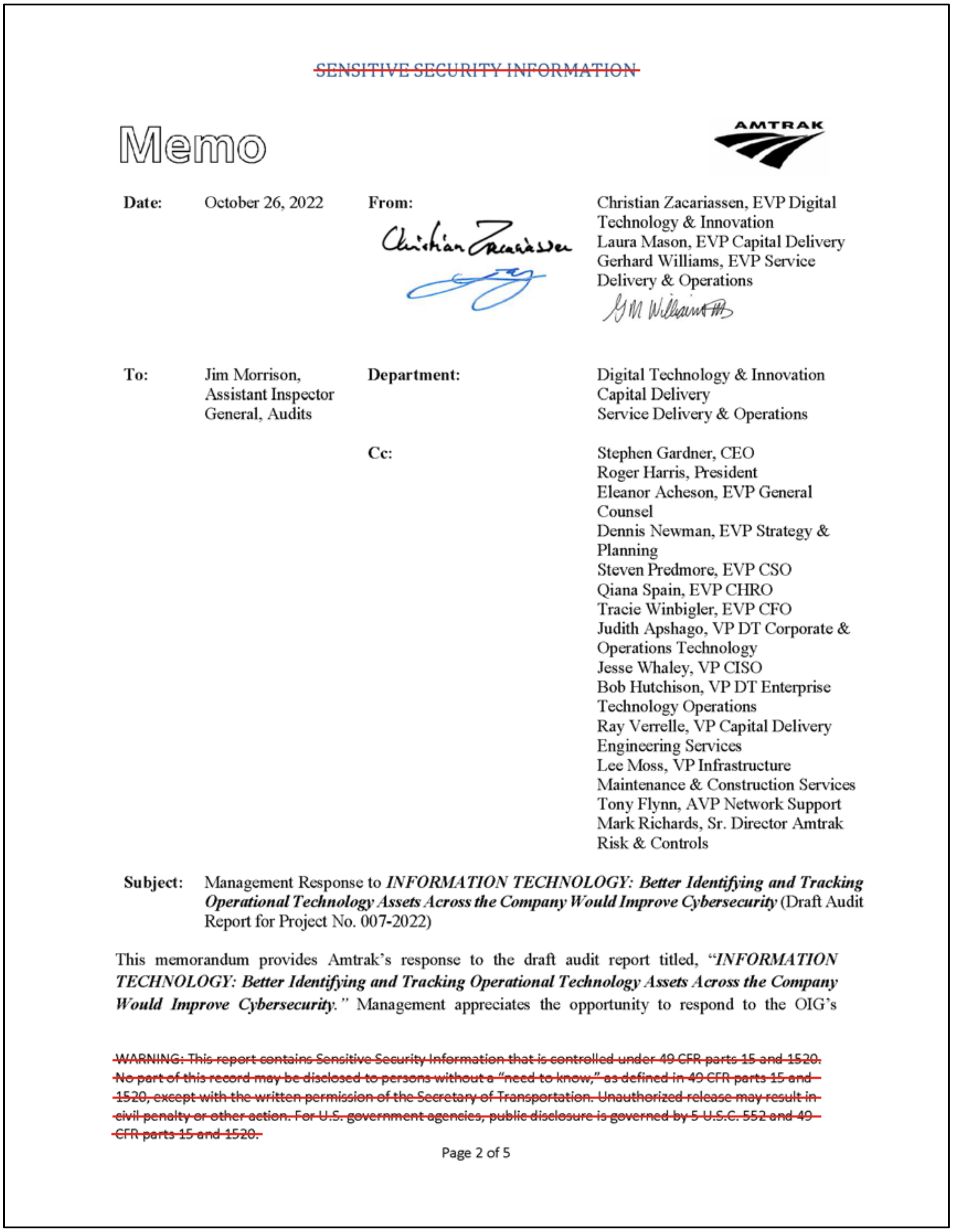
Cover Sheet

For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (8/10) Reference: 49 CFR § 1520.13, Marking SSI

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~

Memo

AMTRAK

Date: October 26, 2022

From: Christian Zacariassen, EVP Digital Technology & Innovation
Laura Mason, EVP Capital Delivery
Gerhard Williams, EVP Service Delivery & Operations

Christian Zacariassen

GM Williams

To: Jim Morrison, Assistant Inspector General, Audits

Department: Digital Technology & Innovation
Capital Delivery
Service Delivery & Operations

Cc: Stephen Gardner, CEO
Roger Harris, President
Eleanor Acheson, EVP General Counsel
Dennis Newman, EVP Strategy & Planning
Steven Predmore, EVP CSO
Qiana Spain, EVP CHRO
Tracie Winbigler, EVP CFO
Judith Apshago, VP DT Corporate & Operations Technology
Jesse Whaley, VP CISO
Bob Hutchison, VP DT Enterprise Technology Operations
Ray Verrelle, VP Capital Delivery Engineering Services
Lee Moss, VP Infrastructure Maintenance & Construction Services
Tony Flynn, AVP Network Support
Mark Richards, Sr. Director Amtrak Risk & Controls

Subject: Management Response to ***INFORMATION TECHNOLOGY: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity*** (Draft Audit Report for Project No. 007-2022)

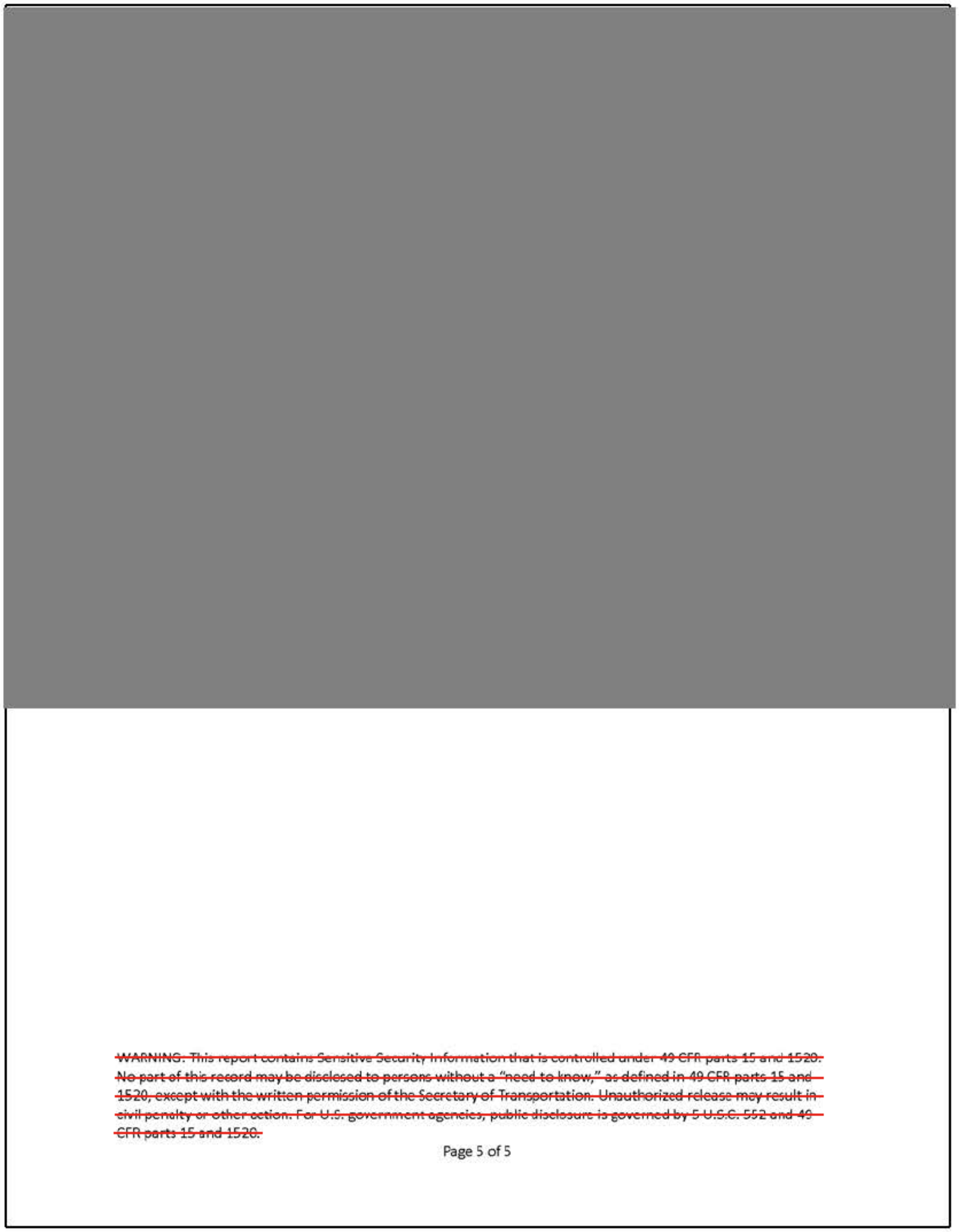
This memorandum provides Amtrak's response to the draft audit report titled, "***INFORMATION TECHNOLOGY: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity.***" Management appreciates the opportunity to respond to the OIG's

~~WARNING: This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

Page 2 of 5

[redacted]

[redacted]



[redacted]

~~WARNING: This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

Page 5 of 5

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

APPENDIX C

Abbreviations

NIST	National Institute of Standards and Technology
OIG	Amtrak Office of Inspector General
OT	operational technology
PTC	Positive Train Control
the company	Amtrak

APPENDIX D

OIG Team Members

J.J. Marzullo, Deputy Assistant Inspector General, Audits

Anne Keenaghan, Senior Director, Audits

Ashish Tendulkar, Audit Manager

Sheila Holmes, Senior Auditor, Lead

Ursula Sundre, Senior Auditor

Alison O'Neill, Communications Analyst

OIG MISSION AND CONTACT INFORMATION

Mission

The Amtrak OIG's mission is to provide independent, objective oversight of Amtrak's programs and operations through audits and investigations focused on recommending improvements to Amtrak's economy, efficiency, and effectiveness; preventing and detecting fraud, waste, and abuse; and providing Congress, Amtrak management, and Amtrak's Board of Directors with timely information about problems and deficiencies relating to Amtrak's programs and operations.

Obtaining Copies of Reports and Testimony

Available at our website www.amtrakoig.gov

Reporting Fraud, Waste, and Abuse

Report suspicious or illegal activities to the OIG Hotline

www.amtrakoig.gov/hotline

or

800-468-5469

Contact Information

Jim Morrison
Assistant Inspector General
Mail: Amtrak OIG
10 G Street NE, 3W-300
Washington, D.C. 20002
Phone: 202-906-4600

~~**WARNING:** This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~