~~SENSITIVE SECURITY INFORMATION~~

AMTRAK OFFICE *of* INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

Technology:

Opportunities Exist to Improve the Company's Disaster Recovery Practices for Its Operational Technology Systems

OIG-A-2025-003 | January 31, 2025

~~**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.

AMTRAK OFFICE *of* INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

Memorandum

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

From: J.J. Marzullo
Assistant Inspector General, Audits

Date: January 31, 2025

Subject: *Technology: Opportunities Exist to Improve the Company's Disaster Recovery Practices for Its Operational Technology Systems* (OIG-A-2025-003)

Amtrak (the company) uses operational technology (OT) systems[1] to manage equipment that controls train operations, such as communications and dispatching. Disruptions to these systems resulting from a disaster[2]—whether caused by human or technical error, natural disasters, cybersecurity attacks, or physical attacks—could cause train delays and cancellations, revenue losses, and safety risks. For example, in late December 2023, network device failures in one OT system caused multi-hour disruptions to 14 trains on the Northeast Corridor (NEC), which led to revenue losses and reputational damage to the company. One of the company's goals is to continuously improve disaster recovery and system resiliency[3] for all technology systems. These include OT systems, as well as information technology systems, which process business data. Accordingly, our objective was to assess the company's disaster

[1] OT systems monitor and control physical processes or interact with the physical environment. They 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.

[2] In the technology industry, a disaster can be any unexpected problem that results in a slowdown, interruption, or failure in a key system or network.

[3] Disaster recovery refers to restoring systems in the event of atypical, unplanned events, such as the loss of a data center to a fire or a cybersecurity attack; system resiliency is the ability to continue system operations and resolve day-to-day issues that do not rise to the level of a disaster. We refer to disaster recovery and system resiliency collectively as "disaster recovery," which is common in the technology industry.

~~**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.~~

recovery practices for its OT systems.[4] Our scope included the technical systems, such as servers and network devices, that monitor and control equipment; it did not include the equipment itself, such as radios, signals, and catenary lines.[5]

To address our objective, we reviewed company documents and assessed its controls to mitigate the risk of disruptions to OT systems. We also interviewed company officials in the Digital Technology and Innovation (DT) and Capital Delivery departments. Lastly, we conducted site visits of the company's train control centers in Washington, D.C.; Wilmington, Delaware; Philadelphia, Pennsylvania; New York City; and Boston, Massachusetts. For more information on our scope and methodology, see Appendix A.

SUMMARY OF RESULTS

The company has developed a strategy for improving disaster recovery for its technology systems but has not fully implemented it across its four OT systems—Train Dispatch, Electric Traction, Positive Train Control (PTC), and Communications and Signals (C&S). In particular, the company does not fully backup all OT data or have redundant hardware for these systems. In addition, it does not maintain fully functional alternate work sites, conduct routine disaster recovery exercises, or routinely replace outdated devices, contrary to industry standards.

The company has not fully implemented its strategy because of three factors:

- **Disaster recovery efforts are fragmented.** Responsibility for disaster recovery is fragmented across four groups under the DT and Capital Delivery departments. Despite this fragmentation, the company has no mechanism to ensure consistent coordination between all groups with disaster recovery responsibilities.

[4] We previously reported on the company's disaster recovery efforts for its information technology systems. Accordingly, information technology systems were outside the scope of this review. See: *Information Technology: Opportunities Exist to Improve the Company's Ability to Restore IT Services After a Disruption* (OIG-A-2018-010), September 18, 2018.

[5] Catenary lines are an overhead arrangement of poles and wires that supply electricity to trains. Notably, the company experienced failures on the NEC this past summer due to aging catenary equipment, but this equipment was outside the scope of our review.

- **Disaster recovery plans are not comprehensive.** The company has not developed comprehensive disaster recovery plans for its four OT systems. Instead, when disruptions occur, the company relies on the institutional knowledge of staff to recover these systems in a timely manner.
- **Incomplete plan to replace or refresh outdated OT devices.** The company has not developed a complete plan with milestones for replacing or refreshing OT devices that are outdated—that is, no longer vendor-supported. The company recognizes this, but company staff told us they have not fully replaced or refreshed old devices because they are still functioning, among other reasons. This approach, however, is not sustainable, as outdated devices will eventually fail.

Without increased focus on its disaster recovery strategy and execution, the company leaves itself vulnerable to OT disruptions that could cause train delays, revenue losses, and safety risks. To reduce the risk of disruption to its OT systems, we recommend the company establish a mechanism to ensure coordination across all groups with disaster recovery responsibilities. We also recommend that the company develop, document, and implement a comprehensive disaster recovery plan for each OT system and begin implementing a plan to replace outdated devices.

In commenting on a draft of this report, the company agreed with our recommendations and described ongoing actions and actions it plans to take by September 30, 2026, to address them. For management's complete response, see Appendix E.

BACKGROUND

The company uses the following four types of OT systems[6] for its train operations:

- **Train Dispatch systems** allow personnel to control the equipment that dispatches and monitors trains. The company has seven distinct Train Dispatch systems with servers and workstations installed across nine locations. For additional details on company locations, see Appendix B.

- **Electric Traction systems** allow personnel to control the flow of electricity from suppliers through substations, on to overhead catenary lines, and ultimately to the electric trains that travel on the NEC. The company has two Electric Traction systems, with servers and workstations installed across seven locations. For additional details on these locations, see Appendix C.

- **PTC systems** monitor train movements and control the equipment that automatically slows or stops trains to help prevent accidents. On the NEC, the company's *Acela* and regional trains, along with some other railroads, use the PTC Advanced Civil Speed Enforcement System (ACSES) system, which has servers and equipment installed at two company locations.[7]

- **The C&S system** includes an array of networking hardware that helps carry radio and data transmissions for the Train Dispatch, Electric Traction, and PTC ACSES systems. The system also allows train dispatchers to communicate remotely with signaling equipment that controls the movement of trains along tracks. The company has networking hardware and equipment installed at five primary locations and along the railway track.

[6] [redacted]

[7] We limited our review to company-managed OT systems. Accordingly, we excluded the company's other two PTC systems—Interoperable Electronic Train Management System (I-ETMS) and Incremental Train Control System (ITCS)—which vendors manage.

~~**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.~~

Roles and responsibilities. Two departments are responsible for disaster recovery of the company's OT systems:

- **The DT department**, led by the Executive Vice President for Digital Technology and Innovation, includes the Corporate and Operations Technologies group, which is responsible for overseeing disaster recovery efforts for the Train Dispatch systems. Also within DT, the Technology Operations Management group is responsible for creating a framework for disaster recovery capabilities, and the Information Security group is responsible for overseeing the company's cybersecurity efforts and ensuring departments meet disaster recovery requirements.

- **The Capital Delivery department**, led by the Executive Vice President for Capital Delivery, includes the Engineering Services group, which has three teams responsible for overseeing disaster recovery efforts for the Electric Traction, PTC, and C&S systems.

Standards. The National Institute of Standards and Technology (NIST) publishes standards that provide methods for organizations to restore system operations quickly and effectively following a disruption. These standards suggest that organizations back up their data, develop redundant capabilities, set up fully functional alternate work sites, perform regular disaster recovery exercises, and replace devices before they are outdated.[8]

Company policies. DT has also established policies and standards relevant to disaster recovery. For example, one policy requires company departments to develop and implement disaster recovery plans,[9] while another requires DT, in coordination with

[8] NIST, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, September 2020; NIST, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34 Revision 1, May 2010; and NIST, *Guide to Operational Technology Security*, Special Publication 800-82r3, September 2023.

[9] Amtrak Policy, Information Security Roles and Responsibilities, May 24, 2022.

other departments, to ensure recovery of critical information systems, including OT systems.[10]

COMPANY MADE PROGRESS IN ADVANCING FOUNDATIONAL ELEMENTS OF DISASTER RECOVERY

To its credit, the company has developed a strategy for improving disaster recovery for its technology systems. The strategy, which aligns with NIST standards, calls for DT and other departments to have formal disaster recovery plans and documented procedures. It also calls for departments to regularly test the most critical technology systems—including the OT systems it determined are critical to business operations—to ensure the company can recover them after a disruption. Having such a strategy provides a consistent framework and clear direction for the company to implement disaster recovery capabilities across its technology systems.

In addition, the company completed several initiatives to improve the reliability of its OT systems. For example, previously a vendor had managed two of the company's seven train dispatch systems, but as of March 2024, the company is managing all seven systems internally, which reduces the complexity of implementing disaster recovery practices. As of October 2024, the company also had efforts underway to update and centralize all its Electric Traction systems, which it expects to complete by March 2025. Lastly, in early 2024, the company, with the help of a vendor, migrated critical technology components for one of the three PTC systems to the cloud, thus improving its system availability and reliability.

COMPANY HAS NOT FULLY IMPLEMENTED ITS DISASTER RECOVERY STRATEGY FOR OT SYSTEMS

Notwithstanding this progress, the company has not fully implemented the practices it established in its disaster recovery strategy—and that NIST standards call for—across all four OT systems. Specifically, we identified shortcomings in the following five areas:

[10] Amtrak Policy, Server Policy and Standard, May 23, 2022.

- **System backups.** For two of the four systems—Electric Traction and C&S—the company does not fully back up its data, contrary to what NIST standards and the company's strategy call for. For example, although staff managing the C&S system back up data at the company's train control centers, they do not regularly back up data for all 1,371 field network devices that transmit train status information to nearby stations. Company staff acknowledged that if any of these devices were to fail, it would take them more time to recover than if they had a current backup of the data. Further, until staff recovered or replaced the affected devices, approaching trains may have to operate at slower speeds because operators would not have the comprehensive, real-time, mission-critical data they need to operate trains safely at regular speeds. If multiple field network devices were to fail—in the event of a cyberattack, for example—the absence of complete backups would increase the time it takes to recover them, potentially resulting in multiple train delays.

- **System redundancy.** The four systems do not have duplicate hardware and other technology needed to continue operations if the primary system fails—a concept called "system redundancy." NIST standards and the company's strategy call for system redundancy and failover capabilities in such instances. [redacted] Company staff stated that if this happens, it could take several hours to restore PTC operations. During such an outage, the company's operating rules require locomotive engineers to take manual control of trains to ensure safety, resulting in lower speeds and thus train delays.[11] [redacted]

[11] As we have reported in the past, when PTC is unavailable, trains have to abide by traditional practices to ensure that operations are safe, such as obeying signaling systems and rules that guide locomotive engineers. See: *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.

~~**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.~~

- **Alternate work sites.** [redacted][12] [redacted]

- **Disaster recovery exercises.** For three of the four systems, the company does not conduct routine disaster recovery exercises, as NIST standards and the company's strategy call for. For the fourth system—Train Dispatch—DT staff recently performed such exercises but did not do so consistently across all locations. Without routine disaster recovery exercises, company staff may not be familiar with the restoration steps they would need to take in the event of a disruption, potentially resulting in impacts to train operations.

- **Outdated OT devices.** For three of the four systems, the company relies on devices that have reached the end of their useful lives, contrary to NIST standards. Most significantly, the vendor no longer supports 19 of the 100 devices the company relies on for its C&S network. Of these, 14 have not been supported in five years, and one of the remaining five has not been supported for over 10 years. Outdated OT devices are susceptible to failures and increased cybersecurity vulnerabilities.

For additional details on weaknesses in these five areas, see Appendix D.

[12] [redacted]

THREE FACTORS CONTRIBUTED TO THESE WEAKNESSES

The company has not fully implemented its disaster recovery strategy for OT systems because of three factors. First, at a high level, responsibility for disaster recovery is fragmented across departments. Second, the company has not developed comprehensive disaster recovery plans for the four systems. Lastly, at a tactical level, the company has not fully planned for how it will replace outdated OT devices.

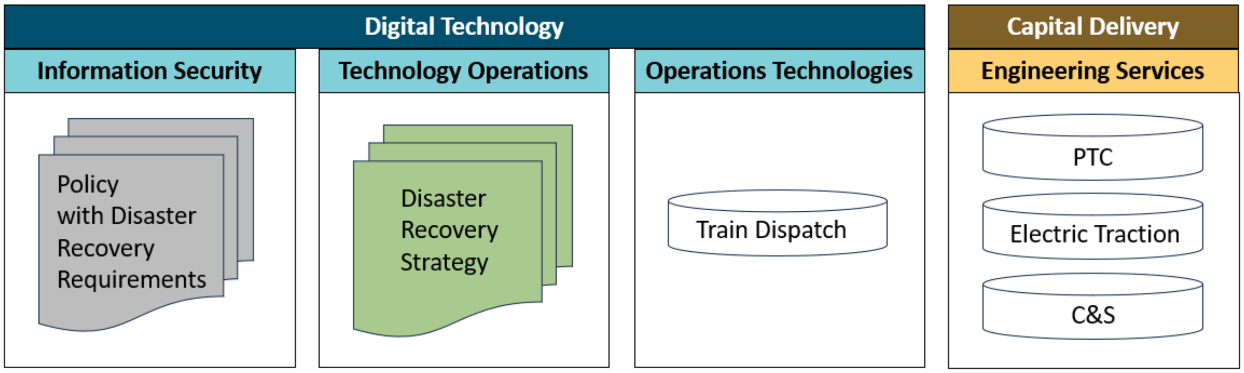
Disaster Recovery Efforts Are Fragmented

Four groups under the DT and Capital Delivery departments share responsibility for implementing the company's disaster recovery strategy:

- **The Technology Operations group** within DT developed the company's disaster recovery strategy.
- **The Information Security group** within DT has responsibilities outlined in policy for overseeing disaster recovery efforts across the company.
- **Two groups—Operations Technologies** in the DT department and **Engineering Services** in the Capital Delivery department—are responsible for managing the four OT systems, including implementing disaster recovery practices.

Figure 1 depicts those responsible for OT systems.

Figure 1. Disaster Recovery Responsibilities for OT Systems



Source: OIG analysis of company policies, disaster recovery strategy, and other documents, as well as interviews with company officials

Despite this fragmentation, the company has no mechanism to ensure consistent coordination between all groups with disaster recovery responsibilities. Leading practices suggest that an effective coordinating mechanism will help ensure consistent efforts and common goals across groups. Without such a coordinating mechanism, we identified the following challenges:

- **Varying priorities.** DT and Capital Delivery staff told us that the groups managing OT systems recognize the importance of providing immediate technical support during system failures, but aspects of implementing the company's disaster recovery strategy—such as conducting routine disaster recovery exercises—need clarification or fall outside their primary responsibility. Accordingly, the groups varied in how much priority they placed on these ancillary tasks.

- **Limited communication.** The Technology Operations group has not effectively communicated the practices outlined in the strategy it developed. For example, two of the four OT system owners told us that they were not aware of the practices the company expects them to implement.

- **Requirements not reviewed.** DT policy establishes the Information Security group as responsible for ensuring company departments meet disaster recovery requirements, which include developing plans and setting up alternate work sites. Its staff, however, told us they do not check to ensure other departments meet these requirements because Technology Operations—in coordination with the two groups that manage the OT systems—is ultimately responsible for doing so. Information Security staff told us that they are in the process of revising the policy to reflect Technology Operations' responsibilities, but as of October 2024, the policy had not been updated. In the meantime, neither Technology Operations nor Information Security are ensuring disaster recovery requirements are met.

With a more effective coordinating mechanism, the company could help ensure all the groups responsible for implementing disaster recovery are aware of their responsibilities and appropriately prioritizing them.

Disaster Recovery Plans Are Not Comprehensive

The company has not developed and implemented comprehensive disaster recovery plans for the four OT systems, as the company's strategy and NIST standards call for. According to NIST, disaster recovery plans help establish how organizations should back up data and who to communicate with in case of a disruption, as well as provide details about alternate processing facilities. The standards also call for a process to ensure these plans are tested, updated frequently, and are a part of everyday operations. Instead of documented plans, however, the company relies on the institutional knowledge of staff to recover these systems in the event of a disruption.

During our review, the company started drafting disaster recovery plans for two of the four systems—Electric Traction and C&S. It has not, however, completed—or therefore implemented and tested—these plans to ensure they are effective in mitigating the risk of a disaster and responding in the event of one. Without comprehensive disaster recovery plans, the company's approach will continue to be reactive and rely on the commitment and institutional knowledge of its staff, instead of the more proactive, repeatable approach that a plan would provide.

Incomplete Plan to Replace or Refresh Outdated OT Devices

The company has not developed a complete plan with milestones for replacing or refreshing OT devices that are outdated—that is, no longer vendor-supported. The company recognizes that it relies on outdated devices, but company staff told us that they hesitate to replace these devices because (1) the devices are still working, and (2) there are inherent challenges when introducing new devices to OT systems, such as the availability of resources and operational downtime. This approach, however, is not sustainable, as outdated devices will eventually fail and likely cause a system disruption. For example, on New Year's Eve in 2023, 28 outdated networking devices in the C&S system failed, causing a 15-hour system disruption that led to 14 train cancellations on the NEC.

NIST standards call for organizations to assess the state of technology devices and replace or refresh them when they present an operability risk. In the case of the New Year's Eve 2023 disruption, company staff told us that they were aware that the network devices were outdated before the disruption occurred, but they did not prioritize replacing them over other assets. Nonetheless, these staff recognize the importance of replacing outdated equipment and agreed that a technology refresh plan could help them proactively identify, track, and replace such devices.

CONCLUSIONS

Disruptions to OT systems could cause train delays, revenue losses, and safety risks. The company has created a strategy for improving its disaster recovery practices, but it has not fully implemented it across the four OT systems. Establishing a mechanism to ensure coordination of disaster recovery responsibilities, developing comprehensive plans, and implementing a technology refresh plan to replace outdated devices would reduce the risk of disruption to OT systems.

RECOMMENDATIONS

To reduce the risks of disruption to OT systems, we recommend that the company's Executive Vice President for Digital Technology and Innovation, in coordination with other departments, as appropriate, take the following actions:

1. Establish a mechanism to ensure that groups with disaster recovery responsibilities prioritize and enforce the company's strategy and effectively communicate and coordinate with each other.
2. For each OT system, develop, document, and implement a comprehensive disaster recovery plan that includes a process to keep the plan current.
3. Develop and begin implementing a technology refresh plan with milestones for replacing outdated OT devices.

MANAGEMENT COMMENTS AND OIG ANALYSIS

In commenting on a draft of this report, company executives agreed with our recommendations and described ongoing and planned actions to address them, which we summarize below.

- **Recommendation 1**. Management agreed with our recommendation to establish a mechanism to ensure that groups with disaster recovery responsibilities prioritize and enforce the company's strategy and effectively communicate and coordinate with each other. Management stated that it will establish a cross-functional program to oversee and coordinate disaster recovery activities for the four OT systems. It also stated that this program will help review roles and responsibilities, improve communications, and coordinate funding needs to meet the goals of the company's disaster recovery strategy. The target completion date is September 30, 2025.

- **Recommendation 2.** Management agreed with our recommendation to develop, document, and implement a disaster recovery plan for each OT system. Management also stated that it will conduct a detailed disaster recovery capability assessment for OT and develop a roadmap to fill gaps and to achieve the goals of the company's disaster recovery strategy. The target completion date is September 30, 2026.

- **Recommendation 3.** Management agreed with our recommendation to develop and begin implementing a technology refresh plan with milestones for replacing outdated OT devices. Management noted its ongoing prioritization of OT asset replacement and stated that it will develop a multi-year plan with objectives, milestones, and funding requests to replace outdated OT devices, which it will prioritize based on business risk. The target completion date is June 30, 2026.

For management's complete response, see Appendix E. Management also provided technical comments, which we have incorporated in this report as appropriate.

APPENDIX A

Objective, Scope and Methodology

This report provides the results of our review of the company's efforts to reduce the risk of disruption to its OT systems. Accordingly, our objective was to assess the company's disaster recovery practices for its OT systems. To address our objective, we reviewed NIST standards and compared them to company practices. NIST provides standards for organizations to restore system operations quickly and effectively following a service disruption. These standards include backing up data, developing redundant capabilities, setting up fully functional alternate work sites, performing regular disaster recovery exercises, and replacing devices before they are outdated. We performed our work in Washington, D.C.; Wilmington, Delaware; Philadelphia, Pennsylvania; New York City; and Boston, Massachusetts, from January 2024 through October 2024. Certain information in this report has been redacted due to its sensitive nature.

Our scope included the four OT systems supporting the company's train operations: (1) Train Dispatch, (2) Electric Traction, (3) PTC ACSES, and (4) C&S. We limited our review to company-managed OT systems. Accordingly, we excluded the company's other two PTC systems—Interoperable Electronic Train Management System (I-ETMS) and Incremental Train Control System (ITCS)—which vendors manage. In addition, our scope did not include the mechanical and auxiliary equipment that the OT systems monitor and control, such as radios, signals, and catenary lines. Furthermore, our scope did not include assessing whether the company had developed:

- business continuity plans and processes in the event of a disruption.
- a communication strategy for providing forensic and legal response.
- disaster recovery plans and practices for its information technology systems.

To perform our work, we assessed all six of the company's train control centers. We visited five of these control centers: Washington, D.C., Wilmington, Philadelphia, New York City, and Boston. During our site visits, we observed data backup controls, system redundancy capabilities, and alternate work sites, where applicable. We did not visit the remaining train control center in Chicago, Illinois, because the migration of the company's Train Dispatch system there was underway during our review, but we interviewed the site manager to assess disaster recovery practices.

We interviewed company officials in the DT, Capital Delivery, Facilities Management, and Service Delivery and Operations departments and reviewed draft disaster recovery plans where available. We also reviewed company documents, including DT policies and procedures relevant to disaster recovery. For example, a DT policy outlining roles and responsibilities states that the company departments managing OT systems should develop and implement disaster recovery plans and practices and requires the departments to maintain and test the practices regularly.[13] In addition, a server policy and standard requires DT, in coordination with other departments, to ensure recovery of critical information systems, including OT systems.[14] This policy also describes the requirements for departments to document disaster recovery plans, back up their data, set up alternate sites to continue operations in the event of the loss of a primary facility, and periodically test and verify their capabilities for restoring their information systems.

To assess the company's efforts to keep its OT devices up to date, in addition to interviewing company staff, we requested and reviewed company documentation to understand its plans for replacing outdated OT devices. In particular, for C&S, we reviewed the company's inventory documentation and assessed the vendor's end-of-support date for the devices listed.

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.

[13] Amtrak Policy, Information Security Roles and Responsibilities, May 24, 2022.
[14] Amtrak Policy, Server Policy and Standard, May 23, 2022.

Internal Controls

We reviewed the internal controls the company had in place for disaster recovery processes of its four OT systems. Specifically, we assessed internal control components and underlying principles and determined that the following two internal control areas were significant to our audit objective:

- **Control Environment**. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
- **Control Activities.** Management should develop and implement activities through policies and procedures to ensure that the company achieves its 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 disaster recovery processes
- disaster recovery policies and procedures including draft plans
- methods for communicating disaster recovery practices and challenges across departments
- practices for refreshing or replacing outdated OT equipment

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 inventory data from the company's network backup tool to evaluate company efforts to manage outdated devices. To assess the reliability of these data, we interviewed company staff who created the report. In addition, we performed our own data testing, including checking for out-of-range data and other inconsistencies within the report. We determined that the data were sufficiently reliable for the purpose of our audit.

Prior Reports

In planning and conducting our analysis, we reviewed the following reports:

- *Information Technology: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity* (OIG-A-2023-002), November 7, 2022
- *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: Improving Cybersecurity and Resiliency of Train Control Systems Could Reduce Vulnerabilities* (OIG-A-2019-008), July 9, 2019
- *Information Technology: Opportunities Exist to Improve the Company's Ability to Restore IT Services After a Disruption* (OIG-A-2018-010), September 10, 2018

APPENDIX B

Train Dispatch Systems and Work Site Locations

Train Dispatch Systems	Primary Server Location (Server Name)	Alternate Server Location (Server Name)	Primary Work Site Locations	Alternate Work Site Locations
Train Dispatch System #1	[redacted]	[redacted]	[redacted]	[redacted]
Train Dispatch System #2 New York (Penn Station Central Control - PSCC)	[redacted]	[redacted]	[redacted]	[redacted]
Train Dispatch System #3 New York (Central Electric Traffic Control - CETC-West)	[redacted]	[redacted]	[redacted]	[redacted]
Train Dispatch System #4 New York (Albany-Hudson)	[redacted]	[redacted]	[redacted]	[redacted]
Train Dispatch System #5 (Wilmington/Washington, D.C.)	[redacted]	[redacted]	[redacted]	[redacted]
			[redacted]	[redacted]
Train Dispatch System #6 Chicago (Michigan East and West)	[redacted]	[redacted]	[redacted]	[redacted]
Train Dispatch System # 7 Chicago (Chicago/New Orleans)	[redacted]	[redacted]	[redacted]	[redacted]

Source: OIG analysis of company documents and interviews with OT system owners

~~**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

Electric Traction Systems and Work Site Locations

Electric Traction Systems	**Primary Server** Location (Server Name)	**Alternate Server** Location (Server Name)	**Primary Work Site Locations**	**Alternate Work Site Locations**
Power Director[a]				
Electric Traction System #1 (Mid-Atlantic Division)	[redacted]	[redacted]	[redacted]	[redacted]
Electric Traction System #2 (New York Division)	[redacted]	[redacted]	[redacted]	[redacted]
Electric Traction System #3 (New England Division)	[redacted]	[redacted]	[redacted]	[redacted]
Load Dispatch[b]				
Electric Traction System #1 (Mid-Atlantic Division)	[redacted]	[redacted]	[redacted]	[redacted]

Source: OIG analysis of company documents and interviews with OT system owners

Notes:
[a] A Power Director is a sub-system of the Electric Traction system that manages the distribution of electrical power within their assigned territory on the NEC.

[b] A Load Dispatch is a sub-system of the Electric Traction system that draws electrical power primarily from the utility providers and ensures that it is safely delivered to the company's transmission network on the NEC.

APPENDIX D

Company Practices Compared to NIST Standards for Each OT System

The table below provides a summary of how company practices we reviewed align with NIST standards for disaster recovery.

KEY

○ = Company practice does not align with NIST standard
● = Company practice aligns with NIST standard
N/A = NIST standard is not applicable to the company's system environment

Train Dispatch Systems	
System Backups **NIST Standard:** *Conduct backups of user and system information at a defined frequency. Establish an alternate storage site, geographically distinct from the primary site, that provides controls equivalent to that of the primary site.*	
●	Train Dispatch staff conduct backups for data needed for regulatory reporting at a defined frequency.
●	Data are stored on tapes at the related alternate work site.
●	Train Dispatch systems are backed up during system releases, and most tapes are stored in [redacted] except the [redacted] server backups, which are stored in [redacted].
System Redundancy & Failover **NIST Standard:** *Plan for the transfer of business functions to alternate processing with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing*.	
○	Train Dispatch systems in [redacted] and two of the three systems in [redacted] have no failover servers. If any of those servers have an outage, the train dispatchers would need to operate using a manual process, which is time consuming.
○	The [redacted] and [redacted] locations have the primary and secondary servers located in the same room, which could lead to a loss of operational continuity in a disaster. This presents a single point of failure.
○	There is no monthly failover testing for the uninterruptible power supply (UPS) and generator at the [redacted] in [redacted] This issue was discovered after a power outage in November 2023 caused a disruption to the Train Dispatch system. The company has since been using a temporary UPS but, as of August 2024, does not have a firm replacement date. In [redacted] the generator is tested more often (weekly) due to its advanced age.

System Redundancy & Failover *(continued)* **NIST Standard:** *Plan for the transfer of business functions to alternate processing with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing*.	
●	One system [redacted] has full replication to support failover to the secondary server.
●	Train Dispatch data centers [redacted] have redundant power, generators, and cooling, and most have monthly UPS and generator failover tests.
●	Servers supporting the Train Dispatch systems have multiple processors to manage the system workload and, therefore, have some redundancy capabilities.
Alternate Worksites **NIST Standard:** *Establish an alternate processing site, geographically distinct from the primary site, to permit the transfer and resumption of operations for essential mission and business functions within established recovery time objectives when the primary processing capabilities are unavailable.*	
○	[redacted] systems do not have secondary servers at an alternate site. [redacted] has both primary and secondary servers at its alternate site.
○	If the server in [redacted] fails, the alternate site on [redacted] would not be operational without C&S reconfiguring the maintenance connection to [redacted], and the Train Dispatch team repurposing the backup server in [redacted], which could take several hours and is not sustainable due to insufficient bandwidth.
●	Train Dispatch data centers in [redacted] and [redacted] have alternate processing sites with workstations that can support train dispatchers in scenarios where the servers are still operating at the primary site.
Disaster Recovery Exercises **NIST Standard:** *Execute contingency plan activities to restore organizational mission and business functions, at a defined frequency.*	
○	As of July 2024, disaster recovery tests for the [redacted] site were not performed.
○	The company performed disaster recovery tests for three sites, but its test steps and documentation of results were not consistent across the sites.
●	The company performed disaster recovery tests for the Train Dispatch system in [redacted], [redacted], and [redacted].
●	The Train Dispatch staff switches to an alternate server when installing or upgrading to a new system, assuring the system stays operable—a component of disaster recovery testing.
Outdated OT Devices **NIST Standard**: *Perform preventative maintenance for system components that present an increased risk to organizational operations.*	
●	As of October 2024, all eight Train Dispatch servers were within their contract support dates.

Electric Traction Systems	
System Backups **NIST Standard:** *Conduct backups of user and system information at a defined frequency. Establish an alternate storage site, geographically distinct from the primary site, that provides controls equivalent to that of the primary site.*	
○	The Power Director configuration backup server in [redacted] is located at the same site as the primary server. In addition, the Load Dispatch backup tape in [redacted] is located at the same site as the primary server. This presents a single point of failure.
○	The configurations for the two Load Dispatch servers [redacted] in [redacted] have not been backed up in over four years.
●	Power Director systems in the [redacted] and [redacted] territories are backed up regularly.
System Redundancy & Failover **NIST Standard:** *Plan for the transfer of business functions to alternate processing with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing.*	
○	The Load Dispatch system has a primary and secondary server, but these servers are at one location in [redacted] This presents a single point of failure.
●	The Power Director systems have failover capabilities in the [redacted] and [redacted] territories. Any one of the servers in the [redacted] can serve as a primary for the other. In [redacted], there is a secondary server in [redacted] and in [redacted].
Alternate Worksites **NIST Standard***: Establish an alternate processing site, geographically distinct from the primary site, to permit the transfer and resumption of operations for essential mission and business functions within established recovery time objectives when the primary processing capabilities are unavailable.*	
○	Not all alternate working sites are functional for disaster recovery purposes. [redacted]
●	[redacted], is functional for disaster recovery purposes.
Disaster Recovery Exercises **NIST Standard:** *To determine the effectiveness of the plan, at a defined frequency, execute contingency plan activities to restore organizational mission and business functions.*	
○	Electric Traction staff do not perform disaster recovery exercises.
Outdated OT Devices **NIST Standard***: Perform preventative maintenance for systems that present an in increased risk to organizational operations.*	
○	The outdated Load Dispatch system has not been migrated to the new system. Electric Traction system staff plan to migrate the Load Dispatch system by March 2025.

<table>
<tr><th colspan="2">PTC ACSES System</th></tr>
<tr><td colspan="2"><b>System Backups</b>
<b>NIST Standard</b><i>: Conduct backups of user and system information at a defined frequency. Establish an alternate storage site, geographically distinct from the primary site, that provides controls equivalent to that of the primary site.</i></td></tr>
<tr><td>●</td><td>The PTC ACSES system is backed up to a SharePoint site when there is a change to the configuration settings.</td></tr>
<tr><td colspan="2"><b>System Redundancy & Failover</b>
<b>NIST Standard:</b> <i>Plan for the transfer of business functions to alternate processing with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing</i>.</td></tr>
<tr><td>○</td><td>[redacted]</td></tr>
<tr><td>○</td><td>If the primary server fails, company staff would have to manually configure a server to continue PTC ACSES operations, which could impact train movements on the NEC.</td></tr>
<tr><td>●</td><td>The server for issuing temporary speed restrictions has built-in hardware redundancy.</td></tr>
<tr><td colspan="2"><b>Alternate Worksites</b>
<b>NIST Standard:</b> <i>Establish an alternate processing site, geographically distinct from the primary site, to permit the transfer and resumption of operations for essential mission and business functions within established recovery time objectives when the primary processing capabilities are unavailable.</i></td></tr>
<tr><td>N/A</td><td>The PTC ACSES system does not have operators and therefore does not require alternate worksites.</td></tr>
<tr><td colspan="2"><b>Disaster Recovery Exercises</b>
<b>NIST Standard:</b> <i>To determine the effectiveness of the plan, at a defined frequency, execute contingency plan activities to restore organizational mission and business functions.</i></td></tr>
<tr><td>○</td><td>PTC ACSES staff do not perform disaster recovery exercises.</td></tr>
<tr><td colspan="2"><b>Outdated OT Devices</b>
<b>NIST Standard</b>: <i>Perform preventative maintenance for system components that present an increased risk to organizational operations.</i></td></tr>
<tr><td>○</td><td>Several PTC ACSES devices—such as communication devices on the locomotives and corresponding wayside technology—are at their end-of-life.</td></tr>
</table>

C&S System	
System Backups **NIST Standard***: Conduct backups of user and system information at a defined frequency. Establish an alternate storage site, geographically distinct from the primary site, that provides controls equivalent to that of the primary site.*	
○	Regular backups of C&S's 1,371 RUGGEDCOM switches—which communicate data and are used in industrial networks because of their ability to operate in harsh environments—are not performed because staff do not have a working backup solution for these switches. The last backup was performed in March 2023.
●	Regular backups of all critical C&S Cisco switches are performed.
●	The two critical backup servers are located at separate locations [redacted].
System Redundancy & Failover **NIST Standard:** *Plan for the transfer of business functions to alternate processing with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing.*	
○	The telecommunications bandwidth between the [redacted] is not sufficient to support train dispatch operations if needed in the event of a major disruption.
●	Redundant communication paths for critical C&S components on the NEC are in place.
Alternate Worksites **NIST Standard:** *Establish an alternate processing site, geographically distinct from the primary site, to permit the transfer and resumption of operations for essential mission and business functions within established recovery time objectives when the primary processing capabilities are unavailable.*	
N/A	The C&S system does not have operators and therefore does not require alternate worksites.
Disaster Recovery Exercises **NIST Standard***: To determine the effectiveness of the plan, at a defined frequency, execute contingency plan activities to restore organizational mission and business functions.*	
○	C&S staff do not perform disaster recovery exercises.
Outdated OT Devices **NIST Standard:** *Perform preventative maintenance for systems that present an increased risk to organizational operations.*	
○	As of August 2024, the C&S network relied on 100 Cisco switches; at least 19 of these are no longer supported by the vendor. Of these, 14 have not been supported in five years. One of the remaining five has not been supported in over 10 years.
○	C&S staff purchased and received 50 of the 200 Cisco switches needed to replace switches as they become outdated. A portion of the first 50 have been installed, but C&S staff have not established a firm date for purchasing and installing the remaining 150 switches.

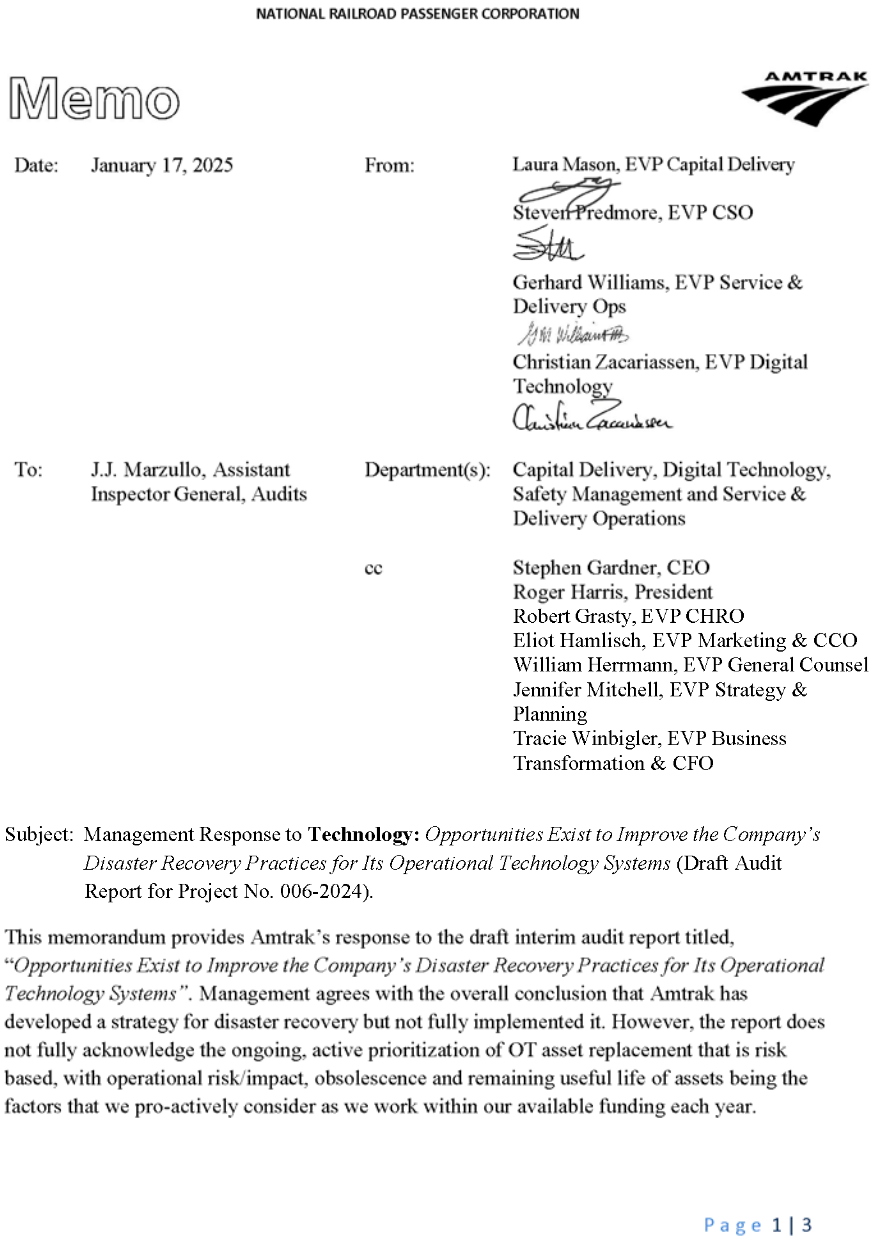
Outdated OT Devices (*continued*) **NIST Standard:** *Perform preventative maintenance for systems that present an increased risk to organizational operations.*	
○	The servers located in [redacted] on the NEC have not been vendor-supported since October 2022, putting the data on these servers at risk. In April 2024, C&S staff initiated the process to purchase two new replacement servers and planned to install them by December 2024.

Source: OIG analysis of company documents and interviews with OT system owners

Amtrak Office of Inspector General
Technology: Opportunities Exist to Improve the Company's Disaster Recovery Practices for Its Operational Technology Systems
OIG-A-2025-003, January 31, 2025

APPENDIX E

Management Comments



NATIONAL RAILROAD PASSENGER CORPORATION

Memo

AMTRAK

Date: January 17, 2025

From: Laura Mason, EVP Capital Delivery
Steven Predmore, EVP CSO
Gerhard Williams, EVP Service & Delivery Ops
Christian Zacariassen, EVP Digital Technology

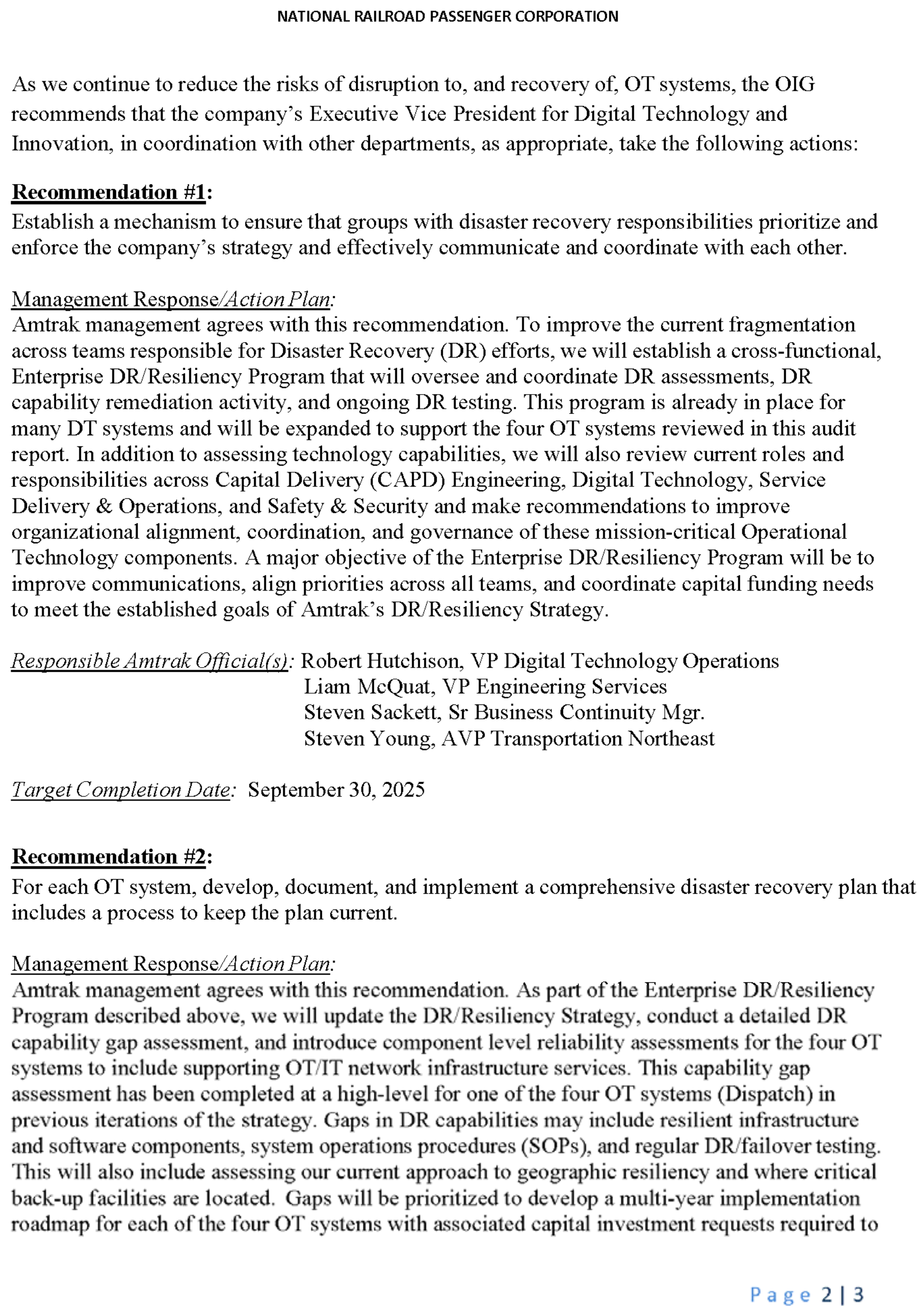
To: J.J. Marzullo, Assistant Inspector General, Audits

Department(s): Capital Delivery, Digital Technology, Safety Management and Service & Delivery Operations

cc Stephen Gardner, CEO
Roger Harris, President
Robert Grasty, EVP CHRO
Eliot Hamlisch, EVP Marketing & CCO
William Herrmann, EVP General Counsel
Jennifer Mitchell, EVP Strategy & Planning
Tracie Winbigler, EVP Business Transformation & CFO

Subject: Management Response to **Technology:** *Opportunities Exist to Improve the Company's Disaster Recovery Practices for Its Operational Technology Systems* (Draft Audit Report for Project No. 006-2024).

This memorandum provides Amtrak's response to the draft interim audit report titled, "*Opportunities Exist to Improve the Company's Disaster Recovery Practices for Its Operational Technology Systems*". Management agrees with the overall conclusion that Amtrak has developed a strategy for disaster recovery but not fully implemented it. However, the report does not fully acknowledge the ongoing, active prioritization of OT asset replacement that is risk based, with operational risk/impact, obsolescence and remaining useful life of assets being the factors that we pro-actively consider as we work within our available funding each year.



NATIONAL RAILROAD PASSENGER CORPORATION

As we continue to reduce the risks of disruption to, and recovery of, OT systems, the OIG recommends that the company's Executive Vice President for Digital Technology and Innovation, in coordination with other departments, as appropriate, take the following actions:

Recommendation #1:
Establish a mechanism to ensure that groups with disaster recovery responsibilities prioritize and enforce the company's strategy and effectively communicate and coordinate with each other.

Management Response/*Action Plan*:
Amtrak management agrees with this recommendation. To improve the current fragmentation across teams responsible for Disaster Recovery (DR) efforts, we will establish a cross-functional, Enterprise DR/Resiliency Program that will oversee and coordinate DR assessments, DR capability remediation activity, and ongoing DR testing. This program is already in place for many DT systems and will be expanded to support the four OT systems reviewed in this audit report. In addition to assessing technology capabilities, we will also review current roles and responsibilities across Capital Delivery (CAPD) Engineering, Digital Technology, Service Delivery & Operations, and Safety & Security and make recommendations to improve organizational alignment, coordination, and governance of these mission-critical Operational Technology components. A major objective of the Enterprise DR/Resiliency Program will be to improve communications, align priorities across all teams, and coordinate capital funding needs to meet the established goals of Amtrak's DR/Resiliency Strategy.

Responsible Amtrak Official(s): Robert Hutchison, VP Digital Technology Operations
Liam McQuat, VP Engineering Services
Steven Sackett, Sr Business Continuity Mgr.
Steven Young, AVP Transportation Northeast

Target Completion Date: September 30, 2025

Recommendation #2:
For each OT system, develop, document, and implement a comprehensive disaster recovery plan that includes a process to keep the plan current.

Management Response/*Action Plan*:
Amtrak management agrees with this recommendation. As part of the Enterprise DR/Resiliency Program described above, we will update the DR/Resiliency Strategy, conduct a detailed DR capability gap assessment, and introduce component level reliability assessments for the four OT systems to include supporting OT/IT network infrastructure services. This capability gap assessment has been completed at a high-level for one of the four OT systems (Dispatch) in previous iterations of the strategy. Gaps in DR capabilities may include resilient infrastructure and software components, system operations procedures (SOPs), and regular DR/failover testing. This will also include assessing our current approach to geographic resiliency and where critical back-up facilities are located. Gaps will be prioritized to develop a multi-year implementation roadmap for each of the four OT systems with associated capital investment requests required to

achieve the Fully Operational DR/Resiliency Capability and reliability/availability targets defined in the DR/Resiliency Strategy.

Responsible Amtrak Official(s): Judith Apshago, VP Corporate and Operations Technology
Robert Hutchison, VP Digital Technology Operations
Liam McQuat, VP Engineering Service

Target Completion Date: September 30, 2026

Recommendation #3:
Develop and begin implementing a technology refresh plan with milestones for replacing outdated OT devices.

Management Response/*Action Plan:*
Amtrak management agrees with this recommendation. DT Operations and Engineering Services will collaborate to develop a comprehensive technology refresh/State of Good Repair (SOGR) plan that addresses all end-of-life/out-of-support OT network devices. This plan will be prioritized based on business risk and will be phased over multiple years. Collaboration across DT and C&S teams is critical to achieve shared objectives of standardizing on common network management tools, support processes, technology standards, and service providers across the Enterprise. This will help increase overall reliability, resiliency, and cybersecurity capabilities. In addition, ensuring all network devices are monitored, patched, and regularly scanned for security vulnerabilities is an important component of this activity. Objectives, milestones, and associated capital funding requests will be developed as part of this Enterprise-level technology refresh plan.

Responsible Amtrak Official(s): Robert Hutchison, VP Digital Technology Operations
Liam McQuat, VP Engineering Services
Jesse Whaley, VP Chief Information Security Officer
Steven Young, AVP Transportation Northeast

Target Completion Date: June 30, 2026

APPENDIX F

Abbreviations

ACSES	Advanced Civil Speed Enforcement System
C&S	Communications and Signals
CETC	Central Electric Traffic Control
CNOC	Consolidated National Operations Center
DT	Digital Technology and Innovation
I-ETMS	Interoperable Electronic Train Management System
ITCS	Incremental Train Control System
NEC	Northeast Corridor
NIST	National Institute of Standards and Technology
OIG	Amtrak Office of Inspector General
OT	operational technology
PTC	Positive Train Control
PSCC	Penn Station Central Control
REA	Railway Express Agency
the company	Amtrak
UPS	Uninterruptible Power Supply

APPENDIX G

OIG Team Members

Anne Keenaghan, Deputy Assistant Inspector General, Audits

Ashish Tendulkar, Director, IT Audits

Sheila Holmes, Audit Manager, IT Audits

Ursula Sundre, Senior Auditor IT Lead

Eli Avevor, IT Auditor

Shannon Briggs, IT 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

J.J. Marzullo
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.~~