

SENSITIVE SECURITY INFORMATION



OFFICE of INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

TECHNOLOGY:

Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats

OIG-A-2024-001 | December 11, 2023

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


This page is intentionally left blank.

~~**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.~~



Memorandum

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

From: Jim Morrison 
Assistant Inspector General, Audits

Date: December 11, 2023

Subject: *Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats (OIG-A-2024-001)*

Like other organizations, Amtrak (the company) faces the inherent cybersecurity risk that employees or contractors are “insider threats” —that is, that they could maliciously or unintentionally use information systems or data in a manner that harms the company. Insider threats may cause more harm and are more difficult to detect than external cyber-attackers because individuals within an organization already have access to systems and data. Our recent investigations identified employees and contractors who misused or took advantage of their system access and exposed sensitive company information. Accordingly, our objective was to assess the effectiveness of company controls to protect its information systems and data from insider threats.

To mitigate insider threats, industry standards identify a broad range of practices—both non-technical and technical—that organizations should follow.¹ We focused on assessing three *technical* practices that are foundational for helping mitigate insider threats. These are (1) monitoring employee and contractor activity on systems and networks to identify concerning behaviors and prevent data loss, (2) responding to information that indicates an insider threat, and (3) implementing controls to restrict unauthorized system access.

¹ Non-technical practices include developing training on insider threats, having strong physical access controls, and implementing practices to screen personnel. Non-technical practices were outside the scope of our review. For more details on our scope and methodology, see Appendix A.

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

To evaluate the extent to which the company follows these practices, we reviewed company policies and procedures; interviewed company officials in the Digital Technology and Innovation department (DT) and other departments; and assessed controls in place to prevent, detect, and address insider threats. We also assessed three major company systems in more depth to determine the extent to which the company restricts unauthorized access to those systems.² For more details on our scope and methodology, see Appendix A.

SUMMARY OF RESULTS

The company's strategy in recent years has focused on hardening its defenses against established and highly disruptive external cyber threats, such as those posed by cyber-criminals and various state and non-state sponsored malicious actors. Internally, however, our work found that the company has opportunities to [REDACTED] strengthen its controls to protect its information systems and data from threats by those who already have legitimate access to them. In pertinent part, we found that the company has not effectively implemented three technical practices that industry standards suggest organizations follow to help mitigate the risk of insider threats. As a result, malicious or negligent insiders could exploit their system access to steal, modify, or expose sensitive data, which poses safety, financial, operational, and reputational risks to the company. Specifically, we identified:

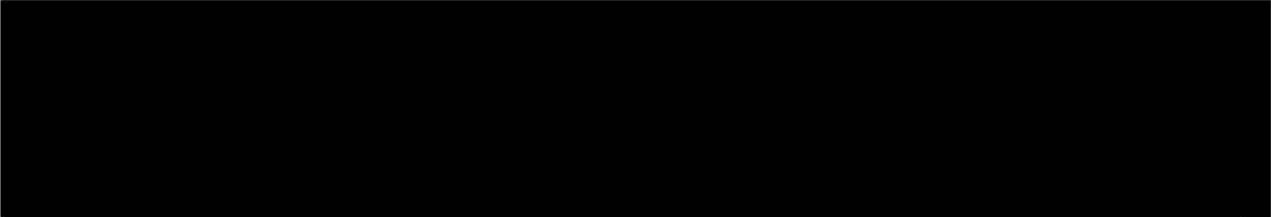
- **Ineffective monitoring of user activity to prevent data loss** [REDACTED]

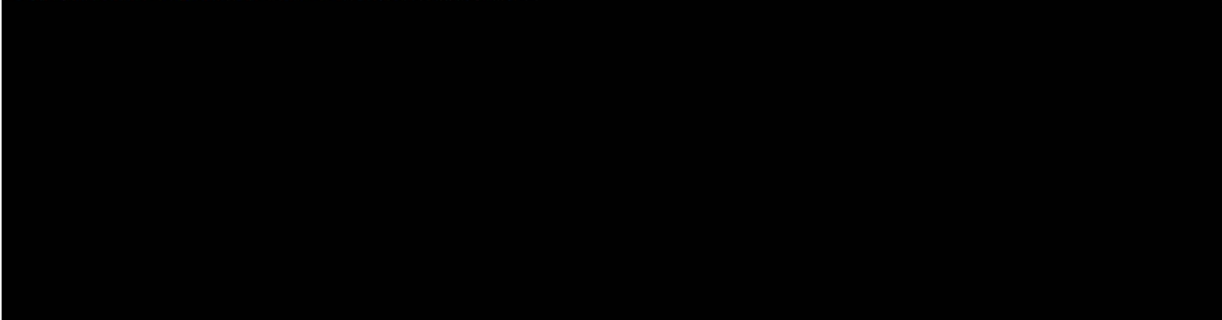
² We reviewed three of the company's non-financial systems: [REDACTED]

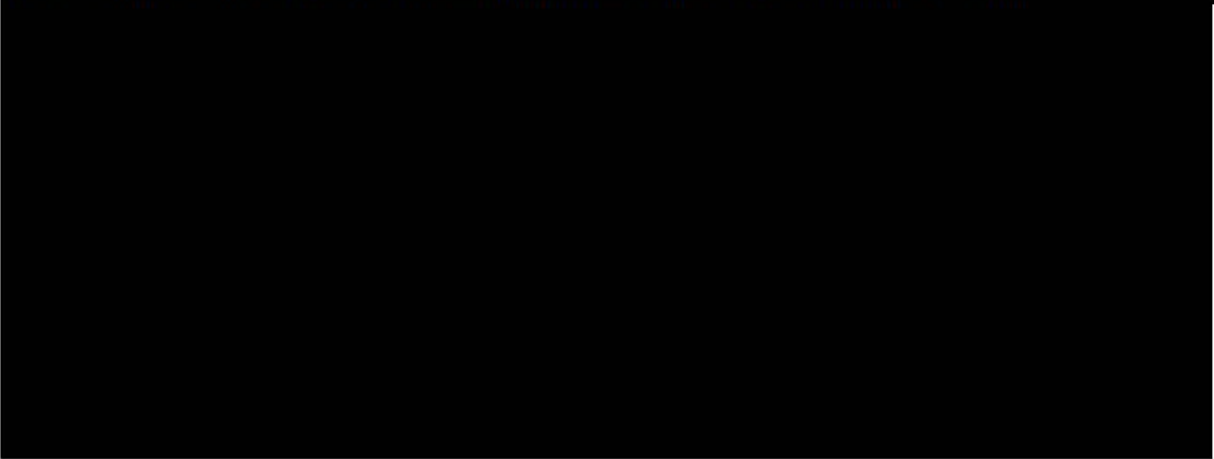
[REDACTED] The company's independent public accountant reviews technology controls for Amtrak's financial systems; therefore, we excluded these systems from our scope. For more information, see Appendix A.

~~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.~~

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

- 
- **Limited response to insider threats.**

- 
- **Inadequate controls to restrict unauthorized access to certain systems.**



To address these shortcomings, we recommend DT coordinate with other departments as necessary to conduct an insider threat risk assessment and, based on its results, implement a plan to better control, monitor, and prevent data loss for its systems. In addition, we recommend the company establish a policy with clear departmental roles for insider threat activities, including responding to insider threat events. Because these efforts may take significant time, we recommend that, in the interim, DT develop a process to track and enforce company access requirements. Lastly, we recommend DT develop a strategy to leverage available tools to strengthen access controls and better

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.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

protect company systems. In commenting on a draft of this report, the company's Executive Vice President for Digital Technology and Innovation agreed with our recommendations and described actions the company plans to take by [REDACTED] to address them. For management's complete response, see Appendix B.

BACKGROUND

The company has more than 340 information technology systems, which process its business data, and operational technology systems, which support its train operations. Any employee or contractor who uses or could use their authorized access to such data and systems to do harm—whether maliciously or unintentionally—is an insider threat.

Standards. The National Institute of Standards and Technology (NIST) publishes industry standards for cybersecurity. These include using technology to detect, alert on, and block unauthorized access to systems and data.³ We focused our review on three technical practices that are foundational for organizations to effectively help mitigate insider threats, as Figure 1 shows.

³ NIST, *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53, Revision 5*, September 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.~~

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

Figure 1. Foundational Technical Practices for Mitigating Insider Threats



Source: *OIG analysis of NIST’s Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53, Revision 5*

The company also has policies and standards relevant to insider threats. For example, its Acceptable Use policy⁴ describes inappropriate uses of the company’s systems and data, including revealing confidential data, using systems without authorization, using cloud storage without authorization, and using personal removable media such as flash drives. In addition, the company’s Identity and Access Management policy⁵ establishes standards to restrict access to company computer systems and networks to valid and authorized users. This policy describes the requirements for creating, monitoring, reviewing, and removing access to company systems to ensure employees and contractors are granted only the access necessary to fulfill their job responsibilities.

Relevant company departments and systems. Insider threats can arise from anywhere within an organization, and each company department may, at any given time, be involved in identifying and responding to these threats. The department most relevant to our review is DT, led by the Executive Vice President for Digital Technology and

⁴ Amtrak Policy, 13.1.6 Acceptable Use Policy, January 31, 2020. During most of our review, version 13.1.6 of the policy was in effect. On June 28, 2023, the company updated its policy to 13.1.7.

⁵ Amtrak Policy, 13.7.1 Identity and Access Management Policy, October 8, 2020. During most of our review, version 13.7.1 of the policy was in effect. On June 27, 2023, the company updated its policy to 13.7.2.

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.

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

Innovation. Within DT, the Technology Operations Management group is responsible for providing employees and contractors with access to company systems that help support its business operations.

DT also includes the Chief Information Security Officer, who is responsible for overseeing the Information Security group and the company’s cybersecurity program. Within the Information Security group, two teams have roles related to insider threats:

- **The Governance, Risk, and Compliance team** is responsible for creating policies, identifying risks, and enforcing company policies related to technology.
- **The Cyber Defense team** is responsible for collecting cyber threat intelligence, managing cyber defense operations, and implementing security tools that have the capability to monitor and prevent cyber threats.

Other company departments are also relevant to addressing insider threats. For example, the company’s Human Resources department includes an office that investigates employees’ potential technology misuse and provides guidance on appropriate disciplinary action, if substantiated. In addition, the Law department provides guidance to the business units on the potential legal risks associated with cybersecurity, data privacy, and confidentiality. Further, the Amtrak Police Department responds to various threats affecting the company and may work with other departments—including our office—to investigate potential insider threats.

As part of our review of the company’s controls, we also assessed the following three major company systems in more depth:

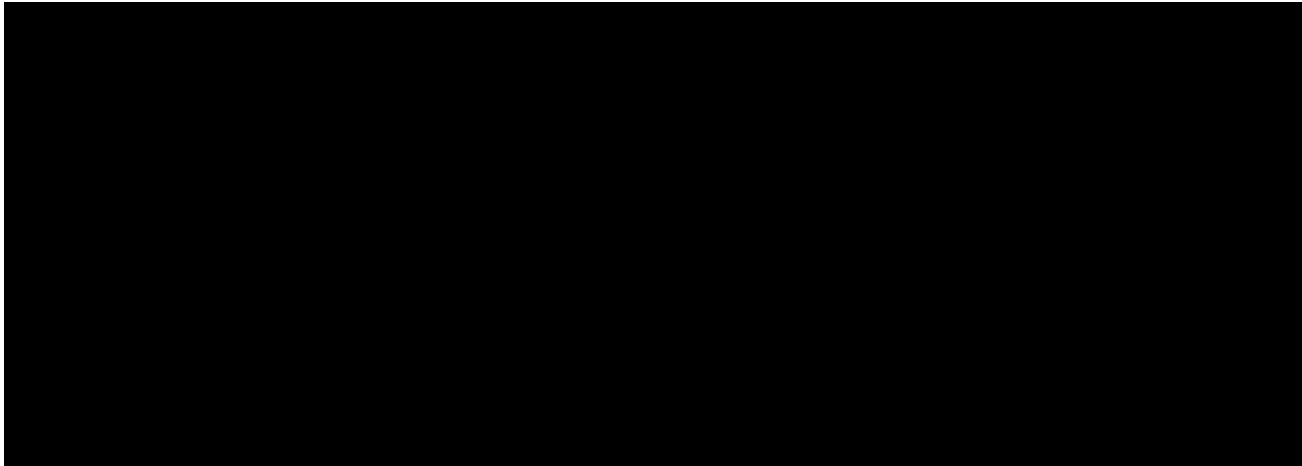
[REDACTED]

[REDACTED]

[REDACTED] Assessing this effort in more detail, however, was outside of the scope of our review.

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.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

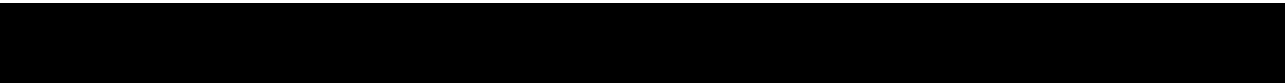


For more details on how we selected these three systems, see Appendix A.

**COMPANY CONTROLS DO NOT EFFECTIVELY PROTECT ITS
INFORMATION SYSTEMS AND DATA FROM INSIDER THREATS**

In recent years, the company’s strategy has been to focus on external cyber threats;⁸ accordingly, it has not fully implemented three foundational technical practices to help mitigate insider threats to its systems and data, which are as follows: (1) monitoring of user activity, (2) responding to information that indicates a potential insider threat, and (3) controlling system access. When measured against those foundational practices, we found shortcomings in the company’s efforts that, collectively, [REDACTED] limit the company’s effectiveness in preventing, detecting, and responding to insider threats.

As a result, malicious or negligent insiders with system access can steal, destroy, modify, or expose sensitive data, which poses safety, financial, operational, and reputational risks to the company. For example, [REDACTED]



⁸ The company’s recent cybersecurity strategies describe efforts to develop capabilities that protect its systems and networks from external cyber threats, including conducting routine penetration tests, gathering cyber threat information, and building its cyber defense operations.

~~**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.**~~

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

[REDACTED]

[REDACTED]. Furthermore, industry research suggests that breaches resulting from negligent and malicious insiders could cost organizations an average of \$485,000 to \$648,000 per incident.¹¹ Addressing the shortcomings we identified in these three technical practices, which we describe in more detail below, could help the company reduce risks insider threats pose.

Monitoring of User Activity is Not Effective to Prevent Sensitive Data Loss

[REDACTED]

Figure 2. [REDACTED]



Source: OIG definitions based on industry terms

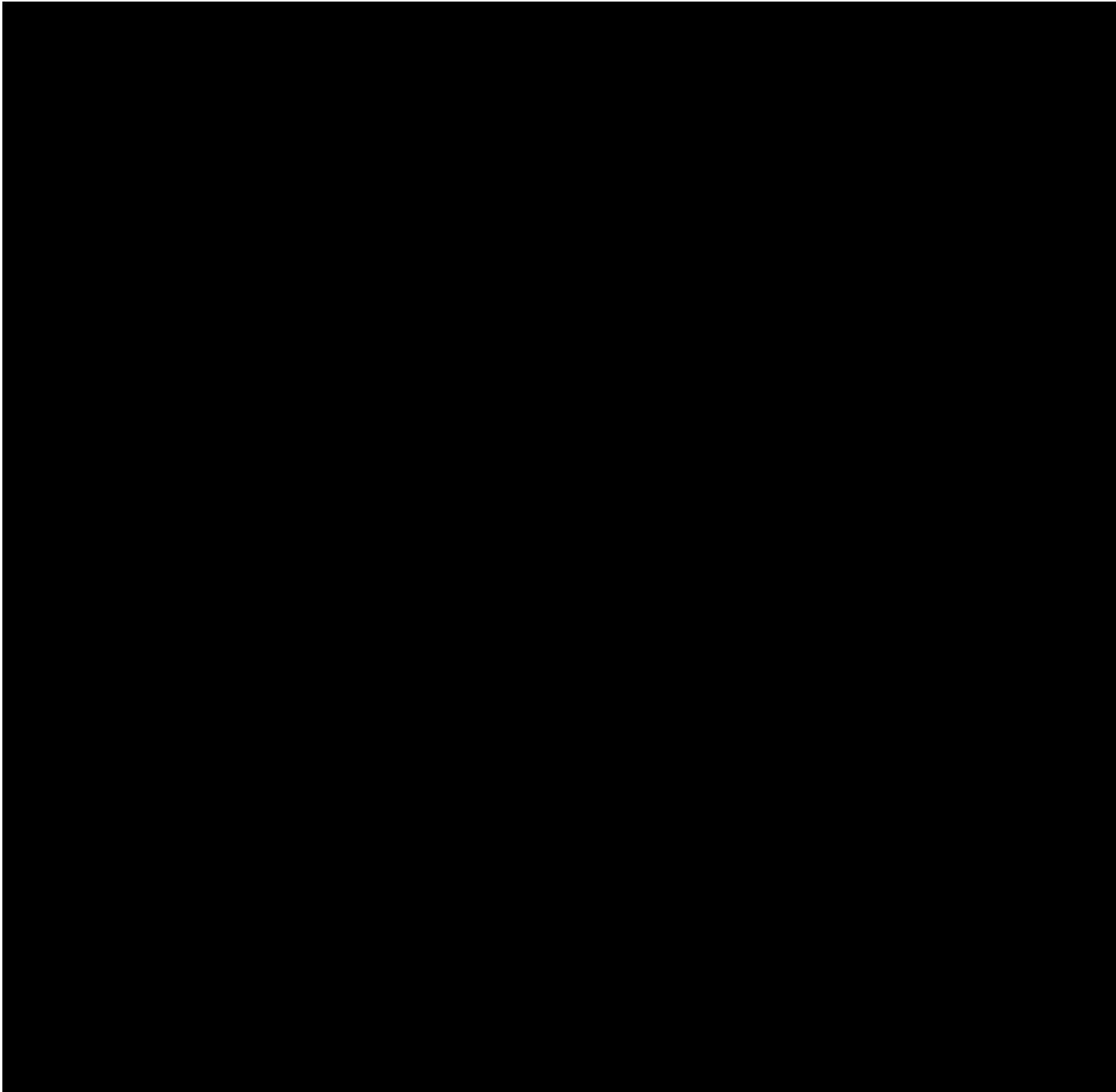
[REDACTED]

[REDACTED]

¹¹ Ponemon Institute, 2022 *Cost of Insider Threats Global Report*.

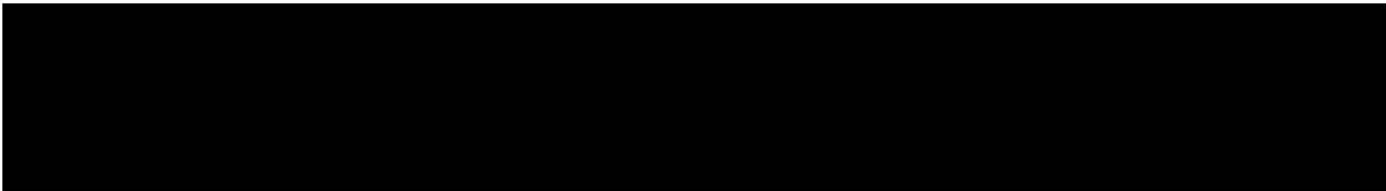
WARNING: This report contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR parts 15 and 1520, except with the written permission of the Secretary of Transportation. Unauthorized 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.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023



~~**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.~~

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023



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.

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

Collectively, for the [REDACTED], DT has not been able to configure its monitoring software to prevent sensitive data loss [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. A risk assessment, with a plan to monitor and block the data and user activities the assessment identifies, would help the company more effectively focus its efforts to mitigate insider threats.

Company Does Not Effectively Respond to Insider Threat Information

DT and relevant departments do not effectively respond to alerts that indicate inappropriate uses of company technology or potential data loss, as industry practices suggest. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

In addition, groups within DT and other departments, such as Human Resources, have not coordinated to determine how to remediate violations—enabling malicious or negligent insiders to continue behavior that may expose company data and increase other cybersecurity risks. Industry practices suggest that insider threat response should include coordination across departments that have a role in activities, such as information security, human resources, operations, and legal counsel.

Company officials told us that it is unclear who is ultimately responsible for directing actions to remediate violations. For example, DT and departmental officials identified each other when we asked who was responsible for responding to insider threat

¹⁷ January 2021 is when the company started tracking such information.

Amtrak Office of Inspector General

Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats

OIG-A-2024-001, December 11, 2023

activities. DT officials told us that they believe that they should not be solely responsible for such activities and that responding to threats should be an enterprise-wide effort. This ambiguity exists because DT and other relevant departments have not established a policy that clearly defines departmental roles and responsibilities for insider threat activities, including responding to insider threats. DT officials told us that they plan to hire an employee who will help define such roles. As of August 2023, however, DT had not yet filled this position.

Controls to Restrict Unauthorized Access to Certain Accounts Are Not Fully Effective

The company does not effectively restrict access to the three major systems we reviewed [REDACTED]. In addition, during our review of these three systems, we identified a separate access-related weakness regarding the company's service accounts, which are system accounts with administrative rights that are not tied to a specific user.

Three selected systems. To its credit, DT established requirements in company policy that, if followed, would reduce the risk of an insider intentionally or unintentionally gaining unauthorized access to all company systems such as the three we reviewed. For example, company policy requires system owners to delete accounts if users do not access them after a certain timeframe and prohibits users from sharing login information to any company system. Our review of the [REDACTED] systems found, however, that these system owners did not consistently adhere to company access requirements, as Figure 3 shows.

~~**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.~~

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

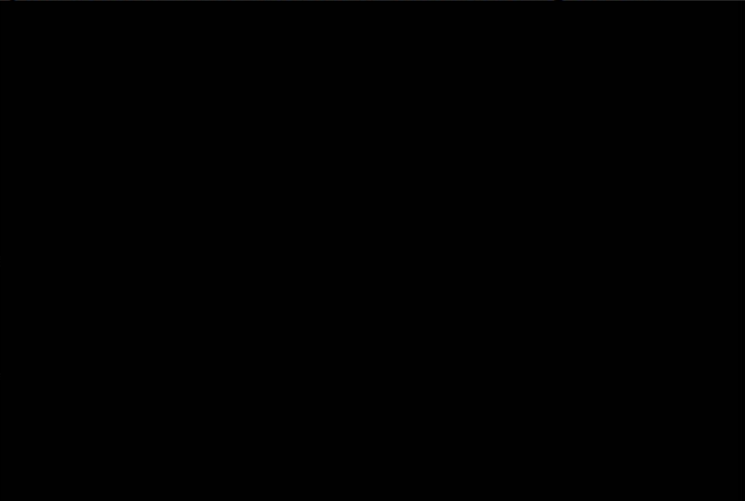
Figure 3. Company Access Requirements Met for Three Selected Systems

Type of Company Requirement

Privileged Access. Company requirements related to managing accounts with elevated system access and capabilities.

Access Revocation. Company requirements related to removing or revoking system access when users no longer need it.

Least Privilege. Company requirements related to limiting system access to only what users need to perform their jobs.



= Met company access requirement

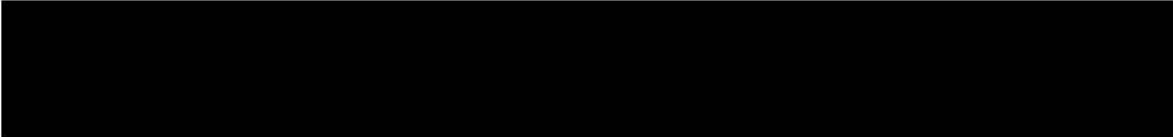


= Did not meet company access requirement

Source: OIG analysis of access controls for selected systems. For more details, see Appendix C.

System owners within company departments, for example, did not regularly assess which users have access to the three systems we reviewed and whether their system rights were commensurate with their job responsibilities, as company policy requires. These system owners told us they were unaware of company access requirements, including regular access reviews.

Inconsistent adherence to company access requirements is occurring because DT has not established a process to track and enforce them for the company’s non-financial systems, including coordinating with system owners to make them aware of and ensure they complete required access reviews. Without such a process, access-control gaps will persist, which increases the risk that insiders could – intentionally or unintentionally – modify, expose, or steal sensitive company data. The following are examples of such increased risks in the three systems we reviewed.

- 

Company requirements include removing accounts after employees depart the

~~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.~~

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

company and ensuring current users' access aligns only with what their duties require and not more.

- [REDACTED]. Industry research finds that most data breaches have a connection to the misuse or compromise of privileged accounts and suggests that organizations minimize their use.
- [REDACTED], we identified:
 - [REDACTED] which are accounts where multiple users share login credentials. Company policy prohibits the use of shared accounts. Sharing login credentials eliminates the ability to identify the specific user of the system.
 - [REDACTED] were also privileged accounts. Company policy requires privileged accounts to have unique usernames and be limited to employees and contractors who require such rights for their jobs. System owners said they could not determine who had used these accounts because, as shared accounts, individual users remain anonymous.
 - [REDACTED]. Company policy requires system owners to delete accounts after 180 days of inactivity. Accounts that employees or contractors are not using provide more openings for a malicious insider or external cyber-attacker to find a way into the system and potentially disrupt train operations. Further, privileged users with broader access than they need could inadvertently change system settings and disrupt train operations.

Establishing a process to track and enforce the company's access requirements would help reduce these risks. Separately, conducting an insider threat risk assessment and

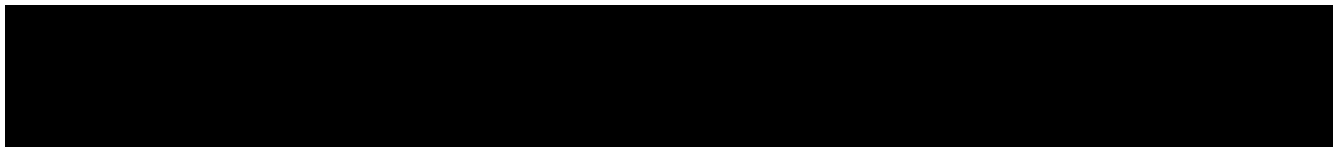
Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

resulting plan, as noted in the section above, would help the company prioritize the access management improvements it needs to address for its systems, including the operational technology systems that support train operations.

Service accounts. During our work, we also found [REDACTED]
[REDACTED]
[REDACTED] The company currently has more than 1,800 service accounts; [REDACTED] of these had [REDACTED], which is not consistent with company policy. Further, in June 2023, DT reviewed password strength for the 491 service accounts it identified as critical to company operations and [REDACTED] did not follow company policy for [REDACTED], and [REDACTED]

[REDACTED] Figure 4 shows these [REDACTED]

Figure 4. [REDACTED] for the Company's Service Accounts



Source: Amtrak OIG analysis of company data

DT has a tool available to centrally manage these accounts and their passwords, which it could use to automatically force [REDACTED] and have the necessary [REDACTED] to meet the company's policy. DT officials told us [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] Accordingly, DT has not established a strategy on how it can implement available access management tools across company systems while minimizing disruption to its operations.

[REDACTED]

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

CONCLUSIONS

With their access to company systems, employees and contractors—whether intentionally or negligently—pose an ongoing threat to the company’s information security. Insiders can misuse their system access to steal, modify, or expose sensitive company data and disrupt train operations leading to potential financial losses, reputational damage, and safety risks to passengers and employees. DT in coordination with other company departments can [REDACTED] strengthen its monitoring, insider threat response, and access management to better protect the company’s systems and data from such threats. Conducting a risk assessment and establishing a plan to put controls into action is a critical first step to effectively direct the company’s insider threat efforts. Developing a policy with clear roles and responsibilities, enforcing the company’s access requirements, and implementing available access management tools to the extent possible would help the company more effectively protect its systems and prevent sensitive data loss.

RECOMMENDATIONS

To protect the company’s information systems and data from insider threats, we recommend the Executive Vice President for Digital Technology and Innovation coordinate with other departments as necessary to take the following actions:

1. Conduct an insider threat risk assessment and determine what data, transfer methods, user activities, and systems are most critical to control, monitor, and block.
2. Based on the results of the risk assessment, develop and implement a plan to better control, monitor, and block identified data and user activities for its systems.
3. Establish a policy that clearly defines departmental roles and responsibilities for insider threat activities, including responding to insider threats.

~~**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.~~

Amtrak Office of Inspector General

Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats

OIG-A-2024-001, December 11, 2023

4. Establish a process to track and enforce access management requirements for the company's non-financial systems, including ensuring system owners are aware of and complete required access reviews.
5. Prioritize and develop a strategy for DT to implement available access management tools across company systems while minimizing disruption to company operations.

MANAGEMENT COMMENTS AND OIG ANALYSIS

In commenting on a draft of this report, the company's Executive Vice President for Digital Technology and Innovation agreed with our recommendations and identified specific actions the company plans to take to address them, which we summarize below.

- **Recommendation 1:** Management agreed with our recommendation to conduct an insider threat risk assessment and determine what data, transfer methods, user activities, and systems are most critical to control, monitor, and block. The company plans to hire a third party to conduct an insider threat risk assessment of the company's critical data, transfer methods, user activities, and systems. The target completion date is [REDACTED]
- **Recommendation 2:** Management agreed with our recommendation to develop and implement a plan to better control, monitor, and block identified data and user activities for its systems. The company plans to develop a project management plan and long-term strategy based on the results of the insider threat risk assessment to implement changes that better protect the company's information systems. The target completion date is [REDACTED]
- **Recommendation 3:** Management agreed with our recommendation to establish a policy that clearly defines departmental roles and responsibilities for insider threat activities. The company plans to establish a cross-departmental committee to define roles and draft an insider threat policy, which management anticipates will cover insider risk indicators, response plans, investigation procedures, and corrective actions. The target completion date is [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.~~

Amtrak Office of Inspector General

Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats

OIG-A-2024-001, December 11, 2023

- **Recommendation 4:** Management agreed with our recommendation to establish a process to track and enforce access management requirements for the company's non-financial systems. The company plans to implement an enterprise-wide policy, compliance process, and training to enforce access management across its critical systems. In addition, management responded that DT has initiated projects to implement a security model that will allow the company to verify user identities and restrict access whenever necessary. The target completion date is [REDACTED]
- **Recommendation 5:** Management agreed with our recommendation to prioritize and develop a strategy for DT to implement available access management tools across company systems while minimizing disruption to company operations. Through its long-term strategy and stakeholder collaboration, the company plans to implement standardized access management tools across its critical systems. The target completion date is [REDACTED]

For management's complete response, see Appendix B.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

APPENDIX A

Objective, Scope and Methodology

This report provides the results of our review of the company's efforts to mitigate the risks associated with insider threats. Our objective was to assess the effectiveness of company controls to protect its information systems and data from insider threats. Our scope included assessing relevant cybersecurity controls from NIST. We reviewed the NIST framework that defines security and privacy controls for information systems and organizations and identified three foundational technical practices related to insider threats. These practices are (1) monitoring of user activity, (2) responding to alerts that indicate inappropriate uses of technology, and (3) restricting access to information systems. We performed our work from February 2023 through August 2023.

To perform our work, we interviewed company officials in DT, Human Resources, Safety and Security, Legal, Finance, Capital Delivery, and Service Delivery and Operations departments to understand their roles and responsibilities for insider threat activities. We also interviewed staff from DT's Information Security group to understand and observe the controls in practice. Lastly, we reviewed the company's Acceptable Use policy and Identity and Access Management policy that cover areas such as the appropriate use of information systems and system access management.

We took the following additional steps specific to each technical practice we reviewed.

To assess the company's monitoring for data loss, we reviewed (and discussed with DT personnel) security tool system configurations for monitoring of user activity for [REDACTED]. For each of the [REDACTED], we assessed whether DT had configured its monitoring software to detect and prevent sensitive data loss.

To assess the company's insider threat response, we interviewed DT personnel to understand how the company evaluated and addressed instances when employees or contractors violated rules for technology use, including potential leaks of company data. We also analyzed user violations data to assess whether DT and other relevant

~~**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.**~~

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

departments followed up when employees violated rules for technology use, including potential sensitive data loss.

To assess the company's access management, we selected a non-generalizable sample of

[REDACTED]. We selected these systems based on information we learned through our interviews and review of the company's database of information systems, its January 2023 disaster resiliency strategy, and its current cybersecurity implementation plan. We considered the following four factors while selecting the three information systems: application type, number of users, criticality, and impact on company operations.

For each of the selected systems, we then assessed whether system owners adhered to the following company requirements that help restrict unauthorized access: (1) managing accounts with elevated access, (2) removing access when users no longer need it, and (3) limiting access to only those users who need it to perform their jobs.

During our review of the selected systems, we learned of a separate issue related to the company's service accounts which are used for system-to-system automated data transfer. For this, we interviewed DT staff to understand the nature and extent of this issue and reviewed security reports [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.

¹⁸ We excluded financial systems from our review because an independent accounting firm tests their access controls as part of the company's annual financial statement audit.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

Internal Controls

We reviewed the internal controls the company had in place to protect its information systems and data from insider threats. Specifically, we assessed internal control components and underlying principles and determined that, in addition to information technology general controls over system access, the following four internal control areas were significant to our audit objective:

- **Control Environment.** Management should oversee the entity's internal control system, establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.
- **Risk Assessment.** Management should identify, analyze, and respond to risks related to achieving the defined 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 internally communicate the necessary quality information to achieve the entity's objectives.

We developed audit work to ensure that we assessed each of these internal control areas. This included reviewing (1) the extent to which the company established clear roles and responsibilities regarding insider threats; (2) how management officials identify, analyze, and respond to significant changes that could impact internal controls; (3) the extent to which the company established policies and procedures for identifying and reporting insider threats; and (4) whether the company departments communicate quality and relevant information to the internal users of its systems.

Regarding information systems controls, we evaluated the design and implementation of controls regarding monitoring, insider threat response, and access management for systems in scope. Given the deficiencies we identified in control design and implementation, testing information systems controls was not included in our review.

~~**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.~~

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

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 collected and examined information from company systems, such as user access lists and system-generated data from security tools, to evaluate the company's controls.

- **User access lists.** We obtained user access lists for the three selected information systems from the DT department, which we used to assess whether the company has implemented controls to mitigate insider threats.
- **System-generated reports.** We requested that company officials generate reports from their security monitoring tools to assess how the company monitors user activity on its network.

To assess the reliability of these data, we interviewed company staff who create the user lists and develop and use the reports. In addition, we performed our own data testing, including checking for out-of-range data and other inconsistencies within the lists and reports. 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:

- *Governance: Quality Control Review of the Independent Audit of Amtrak's Consolidated Financial Statements for Fiscal Year Ended 2022*, (OIG-A-2023-004), December 20, 2022
- *NASA's Insider Threat Program*, (IG-22-009), March 14, 2022
- *Audit of GSA's Insider Threat Program*, (A190016/I/T/F210002), February 17, 2021
- *DHS Science & Technology Has Taken Steps to Address Insider Threats, But Management Challenges Remain*, (OIG-18-89), September 28, 2018
- *USPS Insider Threat Program*, (IT-AR-17-007), September 18, 2017

~~**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.**~~

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

APPENDIX B Management Comments

NATIONAL RAILROAD PASSENGER CORPORATION

Memo



Christian Zacariassen

Date: December 4, 2023

From: Christian Zacariassen, EVP CIO

To: Jim Morrison, Assistant Inspector General, Audits

Department: Digital Technology and Innovation

cc: Stephen Gardner, CEO
 Roger Harris, President
 Eleanor Acheson, EVP General Counsel
 Judith Apshago, VP Chief Digital Officer
 Kuvesh Ayer, VP CPO
 Robert Grasty, EVP CHRO
 Robert Hutchison, VP DT Technology Operations
 Laura Mason, EVP Capital Delivery
 Dennis Newman, EVP Strategy & Planning
 Steven Predmore, EVP CSO
 Gerhard Williams, EVP Service & Delivery Ops
 Jesse Whaley, VP Chief Information Security Officer
 Tracie Winbigler, EVP CFO

Subject: Management Response to **Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats** (Draft Audit Report for Project No. 005-2023).

This memorandum provides Amtrak’s response to the draft interim audit report titled, “*Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats*”. Management agrees with all the noted OIG recommendations below and appreciates the opportunity to provide a response.

To protect the company’s information systems and data from insider threats, the OIG recommends that the Executive Vice President for Digital Technology and Innovation coordinate with other departments as necessary to take the following actions:

Recommendation #1:

Conduct an insider threat risk assessment and determine what data, transfer methods, user activities, and systems are most critical to control, monitor, and block.

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.

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

NATIONAL RAILROAD PASSENGER CORPORATION

Management Response/Action Plan: Management shall contract with a third-party assessment firm to perform a comprehensive insider threat risk assessment of Amtrak critical data, transfer methods, user activities, and systems. This risk assessment shall be performed using industry published frameworks, methodologies, and best practices as a guide. The insider threat risk assessment will identify and provide recommendations to remediate discovered risks utilizing industry best practices.

Responsible Amtrak Official(s): Dale Beauchamp, Sr Director Focused Operations

Target Completion Date: [REDACTED]

Recommendation #2:

Based on the results of the risk assessment, develop and implement a plan to better control, monitor and block identified data and user activities for its systems.

Management Response/Action Plan: Management shall construct a project management plan and long-term strategy based upon the results of the insider threat risk assessment to prioritize and implement appropriate changes that enhance insider threat protections of Amtrak's most critical systems.

Responsible Amtrak Official(s): Dale Beauchamp, Sr Director Focused Operations

Target Completion Date: [REDACTED]

Recommendation #3:

Establish a policy that clearly defines departmental roles and responsibilities for insider threat activities, including responding to insider threats.

Management Response/Action Plan: Management shall create an Insider Risk Management committee consisting of key stakeholders from within Amtrak (DT Cybersecurity, Law, HR, APD, etc.). Leveraging the Insider Risk Management committee, define key roles and create/draft Insider Threat Risk Management policy that includes key insider risk indicators, insider threat response plans, evaluation standards, investigation procedures, and corrective actions. The company hired Dale Beauchamp as Sr. Director of Focused Operations on October 30, 2023, to support the development of the Amtrak Insider Threat Program.

Responsible Amtrak Official(s): Dale Beauchamp, Sr Director Focused Operations

Target Completion Date: [REDACTED]

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

NATIONAL RAILROAD PASSENGER CORPORATION

Recommendation #4:

Establish a process to track and enforce access management requirements for the company's non-financial systems, including ensuring system owners are aware of and complete required access reviews.

Management Response/Action Plan: Management shall implement an enterprise-wide corporate policy, compliance process, and training for the regular review of user access to enforce access management across Amtrak's most critical systems. Digital Technology (DT) has initiated several capital projects to develop and implement Zero Trust Foundations that will give Amtrak a holistic view of users throughout the organization and enable the company to verify identities whenever users attempt to access Amtrak systems and technology resources. Through the implementation of Zero Trust principles, the company may be able to support adherence to the principle of least privilege to grant users the minimum levels of access needed to perform assigned job functions.

Responsible Amtrak Official(s): Tom Enderle, Sr Dir DT Sys Design & Dev Platform Eng
James Mailliard, AVP DT Risk & Compliance

Target Completion Date: [REDACTED]

Recommendation #5:

Prioritize and develop a strategy for DT to implement available access management tools across company systems while minimizing disruption to company operations.

Management Response/Action Plan: Management shall enhance Digital Technology (DT) long-term strategy, including stakeholder collaboration, to extend Amtrak's standardized access management tools across its most critical systems.

Responsible Amtrak Official(s): Tom Enderle, Sr Dir DT Sys Design & Dev Platform Eng
John McSorley, Sr Dir DT Information Security

Target Completion Date: [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.

Amtrak Office of Inspector General
Technology: Amtrak Has Opportunities to More Effectively Protect Its Information Systems and Data from Insider Threats
OIG-A-2024-001, December 11, 2023

APPENDIX C

OIG Analysis of Company Adherence to Access Requirements for Three Selected Systems

Company Requirements OIG Reviewed	
Privileged Access	Privileged accounts were distinct from standard user accounts in the system.
	System owner and the Office of Information Security approved the assignment of elevated rights to the system's privileged users.
	System owner uses the company's ticketing system to request approval for privileged access so that DT can track such access.
	The system did not have any shared accounts where users shared login credentials.
Access Revocation	The system owner deleted dormant accounts that are not already disabled after 180 days.
	The system owner deleted disabled accounts within 30 days.
Least Privilege	System users had access rights commensurate with their job duties.
	System owners reviewed access annually to ensure users did not have more access rights than they should for their job duties.

Source: OIG analysis of access controls for selected systems and company's Identity and Access Management policy

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.

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

APPENDIX D

Abbreviations

DT	Digital Technology and Innovation department
NIST	National Institute of Standards and Technology
OIG	Amtrak Office of Inspector General
the company	Amtrak

~~**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.~~

Amtrak Office of Inspector General
**Technology: Amtrak Has Opportunities to More Effectively Protect Its
Information Systems and Data from Insider Threats**
OIG-A-2024-001, December 11, 2023

APPENDIX E

OIG Team Members

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

Anne Keenaghan, Senior Director, Audits

Ashish Tendulkar, Senior Audit Manager

Sheila Holmes, Senior Auditor, Lead

Ursula Sundre, Senior Auditor, Lead

Eric Elikplim Avevor, Auditor

Nadine Bennett, Associate Legal Counsel

Alison O'Neill, Communications Analyst

~~**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.~~

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.~~