~~SENSITIVE SECURITY INFORMATION~~

AMTRAK

OFFICE *of* INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION

Technology:

Interim Report on the Company's Cloud Computing Practices

OIG-MAR-2025-008 | July 2, 2025

This page intentionally left blank.

~~SENSITIVE SECURITY INFORMATION~~

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: July 2, 2025

Subject: *Technology: Interim Report on the Company's Cloud Computing Practices* (OIG-MAR-2025-008)

During our audit of Amtrak's (the company) cloud computing practices, we identified two pressing cybersecurity issues. We are providing this early alert to bring these issues to the company's immediate attention.[1] Certain information in this report has been redacted due to its sensitive nature.

Like other organizations, the company has been migrating its existing technology systems and data and deploying new systems to the cloud, and its efforts are ongoing. The company uses two cloud service providers—Amazon Web Services (AWS) and Microsoft Azure—to support technology systems that its Digital Technology (DT), Finance, Marketing, Capital Delivery, and Service Delivery and Operations departments use.

[1] We have been performing our audit work in accordance with generally accepted government auditing standards. This interim report is consistent with those standards, which state that providing early communication is important to convey urgency and facilitate prompt corrective action. We will refer to this early alert communication in our final report. This report was prepared in accordance with standards we developed for alternative products.

SIGNIFICANT SECURITY WEAKNESSES IDENTIFIED

Our work to date identified the following security control weaknesses related to external threats that we believe warrant immediate attention.[2]

Limited Controls Exposed Critical Applications to Unauthorized Access

The company's network security controls are limited in preventing unauthorized access to certain applications in the cloud (cloud applications), including some it deems critical to company operations. As part of its recent efforts to protect customer payment information, the company implemented a comprehensive firewall[3] to monitor and filter all data traffic to and from cloud applications that handle customers' credit card data.

[redacted]

A company report identified that the data shared with these actors was limited to generic connection-related information, and company officials told us that no additional data loss occurred. As part of their investigative efforts, Information Security

[2] We assessed the company's security controls for cloud computing by reviewing policies and procedures, interviewing company officials, and examining recent cybersecurity incident reports and other company documents.

[3] A firewall is a security device that monitors the flow of network data and is designed to prevent unauthorized access to and from a private network.

[redacted]

staff (part of the company's DT department) discovered that these servers had been exposed to the internet for several years. In response, the company [redacted]

Information Security Staff's Limited Visibility of Cloud Assets Poses Cybersecurity Risk

Information Security staff do not have full visibility of cloud assets and their activities, which hinders the company's ability to quickly respond to potential cybersecurity incidents. [redacted]

[redacted]

[redacted]

CONSIDERATIONS FOR MANAGEMENT

We plan to continue our audit of the company's cloud computing practices. In the meantime—and before migrating and deploying additional critical company systems, applications, and data in the cloud—the Executive Vice President for Digital Technology and Innovation should consider taking the following immediate actions:

1. Strengthen network security controls to better protect the company's critical cloud-based systems. These actions could include implementing a more comprehensive firewall.
2. Provide Information Security staff full visibility over cloud assets [redacted]

MANAGEMENT COMMENTS AND OIG ANALYSIS

In commenting on a draft of this interim report, the company's Executive Vice President for Digital Technology and Innovation agreed with our considerations for management and identified actions the company plans to take to address them. Management stated that the company will develop a standard for its cloud security measures, enhance firewall configurations, and provide its Information Security staff access to cloud assets based on their job roles. We will assess the company's actions as we continue our work. For management's complete response, see Appendix A. Management also provided technical comments that we have incorporated as appropriate.

Amtrak Office of Inspector General
Technology: Interim Report on the Company's Cloud Computing Practices
OIG-MAR-2025-008, July 2, 2025

APPENDIX A

Management Comments

NATIONAL RAILROAD PASSENGER CORPORATION

Memo

Date:	June 20, 2025	From:	Christian Zacariassen, EVP CIO
To:	John Marzullo, Assistant Inspector General, Audits	Department(s):	Digital Technology
		cc	Roger Harris, President Eliot Hamlisch, EVP Marketing & CCO William Herrmann, EVP Chief Legal and Human Resources Officer (CLHRO) Laura Mason, EVP Capital Delivery Jennifer Mitchell, EVP Strategy & Planning Steven Predmore, EVP CSO Jim Short, Acting SVP Capital Delivery Gerhard Williams, EVP Service & Delivery Ops Tracie Winbigler, EVP Business Transformation & CFO

Subject: Management Response to ***Technology:*** *Interim Report on the Company's Cloud Computing Practices* (Draft Management Advisory Report for Project No. 004-2025).

This memorandum provides Amtrak's response to the draft management advisory report titled, "Interim Report on the Company's Cloud Computing Practices". Management agrees with all the OIG's considerations for management items (observations). The observations provided meaningful input, and we have provided management responses below:

As previously communicated, the OIG plans to continue their audit of the company's cloud computing practices. In the meantime—and before migrating and deploying additional critical company systems, applications, and data in the cloud—the Executive Vice President for Digital Technology and Innovation should consider taking the following immediate actions:

Observation #1:

Strengthen network security controls to better protect the company's critical cloud-based systems. These actions could include implementing a more comprehensive firewall.

Management Response/*Action Plan:* Management acknowledges the importance of strengthening network security controls to better safeguard the company's critical cloud-based systems. As part of this commitment, we will develop a comprehensive standard to guide the implementation of cloud security measures, including enhanced firewall configurations and other

NATIONAL RAILROAD PASSENGER CORPORATION

protective actions. This initiative will ensure alignment with best practices and improve the resilience of our cloud infrastructure.

Responsible Amtrak Official(s): Aaron Mitti, VP Chief Technology Officer
Jesse Whaley, VP Chief Information Security Officer

Target Completion Date: January 31, 2026

Observation #2:

Provide Information Security staff full visibility over cloud assets [redacted]

Management Response/*Action Plan:* Management agrees with the observation that providing Cybersecurity staff full visibility over cloud assets is essential [redacted]

Responsible Amtrak Official(s): Aaron Mitti, VP Chief Technology Officer
Jesse Whaley, VP Chief Information Security Officer

Target Completion Date: November 30, 2025

~~SENSITIVE SECURITY INFORMATION~~

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