



OFFICE *of* INSPECTOR GENERAL  
NATIONAL RAILROAD PASSENGER CORPORATION

## SAFETY AND SECURITY:

Amtrak Has Opportunities to Strengthen Controls over  
High-security Keys

*Certain information in this report has been redacted due to its sensitive nature.*

OIG-MAR-2023-003 | December 12, 2022

This page intentionally left blank.



## Memorandum

**To:** Steve Predmore  
Executive Vice President and Chief Safety Officer

Gerhard Williams  
Executive Vice President, Service Delivery and Operations

**From:** Jim Morrison *[Signature]*  
Assistant Inspector General, Audits

**Date:** December 12, 2022

**Subject:** *Safety and Security: Amtrak Has Opportunities to Strengthen Controls over High-security Keys (OIG-MAR-2023-003)*

High-security keys help protect Amtrak's (the company) critical infrastructure and valuable assets and help provide a safe environment for passengers and employees. These keys provide access to the company's [REDACTED] and other secure areas, as well as those of other railroads.<sup>1</sup> In July 2022, the Amtrak Office of Inspector General (OIG) found that a Florida-based employee violated company policies by attempting to sell high-security switch keys and other railroad keys in an online marketplace.<sup>2</sup> This investigation identified risks related to the rigor of the company's oversight of its high-security keys, especially as it distributes new keys for [REDACTED]  
[REDACTED]

Given these risks, we initiated a review to assess the extent to which the company has controls to manage, distribute, track, and retrieve high-security keys. To accomplish this, we reviewed company policies and procedures regarding key management. We also interviewed officials in three departments regarding their efforts to manage high-security keys—Service Delivery and Operations; Capital Delivery; and Safety, Health, and Environmental. In addition, we conducted site visits where we observed the [REDACTED]<sup>3</sup> For more information on our scope and methodology, see Appendix A.

<sup>1</sup> Although the risks described in this report are not limited to the company's controls over keys, assessing other railroads' controls over their high-security keys was beyond the scope of our review.

<sup>2</sup> *Employee Suspended for Attempting to Sell High-Security Switch Keys (OIG-WS-2022-331)*, July 15, 2022.

<sup>3</sup> We conducted our review in accordance with standards we developed for alternative products.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

## **SUMMARY OF RESULTS**

The company has not consistently implemented controls over the distribution, tracking, and retrieval of its high-security keys, contributing to security and safety risks. It is not feasible, however, for the company to retrieve the thousands of company-issued keys already in the public domain, or to limit the actions of [REDACTED] keys. Nevertheless, the company may reduce its risk by better safeguarding its high-security keys going forward.

**Weak controls contribute to public availability.** Keys are publicly available in part because the company does not exercise strong, industry-recommended controls such as serializing its keys or periodically verifying key-holders. [REDACTED]<sup>4</sup> and weaknesses in their controls—which are outside of the company’s purview—may also contribute to their public availability. Senior officials told us the company has measures in place to largely mitigate serious risks, but the broad availability of these keys could still give bad actors an opportunity to disrupt train operations, causing unnecessary delays and costs.

**Opportunities to reduce risk.** Senior Service Delivery and Operations officials told us it would be futile to try to retrieve keys that departing employees failed to return over the years, and cost-prohibitive to re-key the thousands of locks [REDACTED]

[REDACTED].<sup>5</sup> The company has not, however, formally assessed the risk associated with keys currently in circulation or the practicality and benefit of taking actions to mitigate them. For example, re-keying locks may not be a cost-effective or practical option, but verifying and documenting all current keyholders may be. In addition, because the company had few safeguards in place when it began distributing the new keys that access [REDACTED], it currently cannot account for some of those keys. This lapse underscores the need for strong controls to prevent further loss.

Accordingly, the company may want to consider assessing the cost and risks associated with implementing better controls over high-security keys currently in circulation and implementing those that are practical. In addition, it may want to consider developing a key management policy that institutes new controls and establishing a company-wide

---

<sup>4</sup> [REDACTED]  
[REDACTED]  
[REDACTED]

<sup>5</sup> The company cannot estimate the number of high-security keys that it has issued since its creation, nor the number that are in circulation among current employees.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

mechanism—such as a key management software—to implement them. In commenting on a draft of our report, the Chief Safety Officer agreed with our considerations for management and outlined actions the company plans to take by September 2024 to implement them.

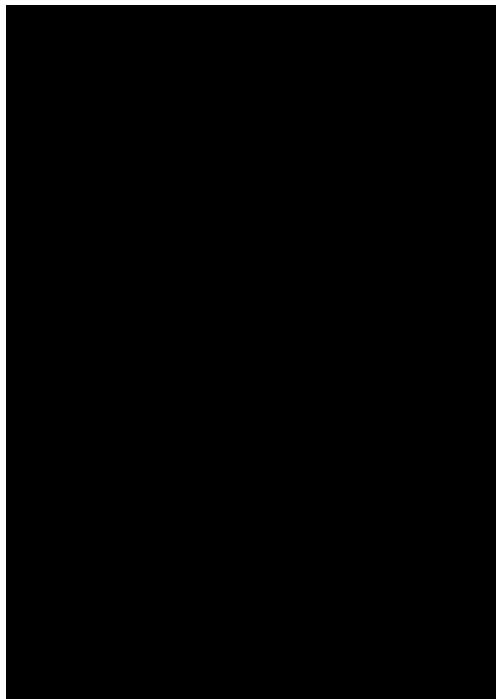
## **BACKGROUND**

Company personnel use several types of keys in their daily work, including some that provide access to critical infrastructure, [REDACTED]

[REDACTED] In some divisions, Material Control field offices (in the Procurement department) store and distribute keys to employees; in other divisions, supervisors distribute keys to their direct reports. We identified the following types of high-security keys:

- [REDACTED] and [REDACTED] keys. These keys secure some of the company's [REDACTED]  
[REDACTED] Additionally, [REDACTED] keys provide access to the company's [REDACTED]  
[REDACTED] Figure 1 shows a [REDACTED] key.

**Figure 1. Company-issued [REDACTED] Key**

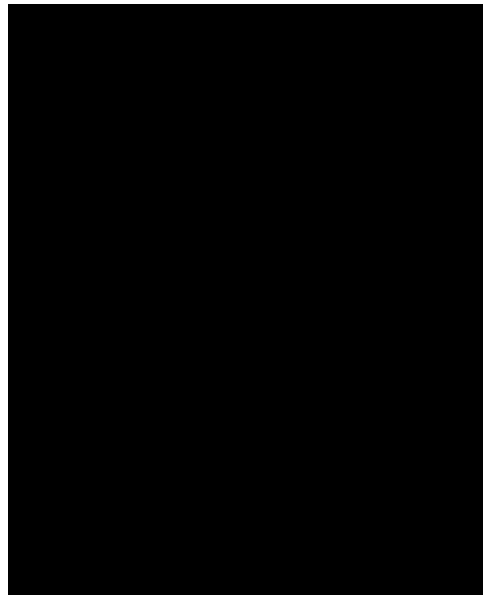


Source: Amtrak OIG, June 2022

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

- [REDACTED] keys. These keys [REDACTED] [REDACTED] shows an [REDACTED]

**Figure 2. Company-issued [REDACTED]**



Source: Amtrak, July 2022

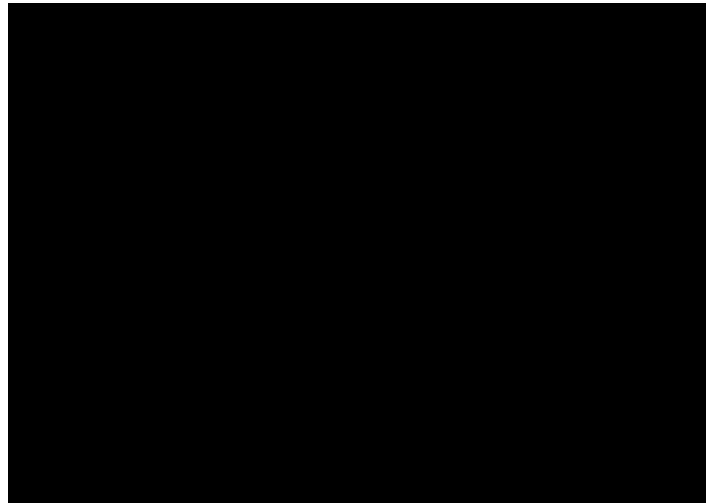
- [REDACTED] keys. These keys, also known as Medeco® keys,<sup>6</sup> [REDACTED] [REDACTED] Figure 3 shows Medeco® keys.

---

<sup>6</sup> The company refers to these as Medeco® keys because Medeco® is the manufacturer.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

**Figure 3. Company-issued Medeco® Keys**



Source: Amtrak OIG, June 2022

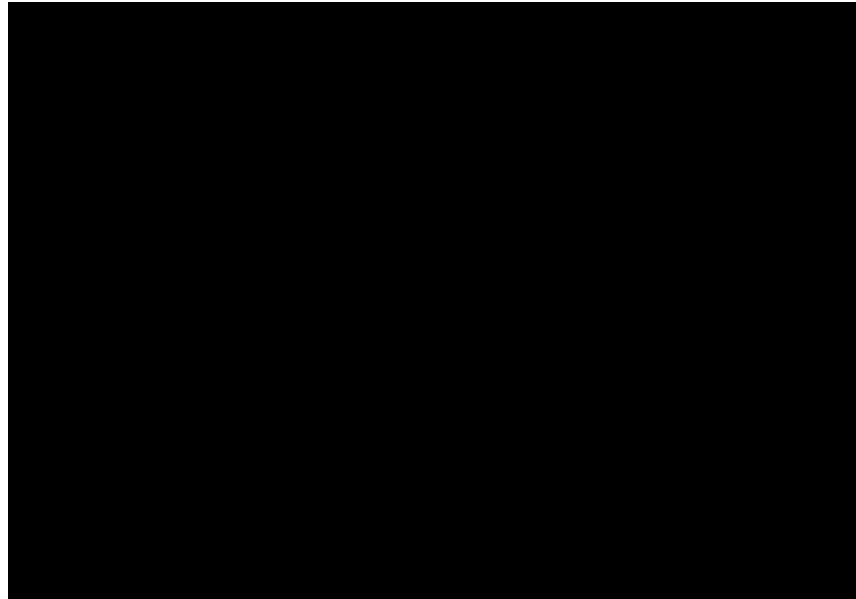
In April 2022, the company began issuing Medeco® keys to support [REDACTED]  
[REDACTED] These keys unlock approximately [REDACTED] to  
prohibit unauthorized access to [REDACTED]<sup>7</sup> Figure 4 shows [REDACTED]  
[REDACTED]  
[REDACTED]

---

<sup>7</sup> The Federal Railroad Administration requires the company to prohibit unauthorized access to [REDACTED]  
[REDACTED]

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

**Figure 4.** [REDACTED]



Source: Amtrak OIG, June 2022

Employees from the Infrastructure Maintenance & Construction Services (IMCS) group (in the Service Delivery and Operations department) will be the main users of the Medeco® keys. Employees in the Transportation group (in the Service Delivery and Operations department) and the Capital Delivery department will also use them. Corporate Security purchases the keys from the manufacturer and distributes them to the departments based on need.

## **COMPANY HAS LIMITED CONTROLS OVER HIGH-SECURITY KEYS**

The company has limited controls governing the distribution, management, tracking, and retrieval of its high-security keys.

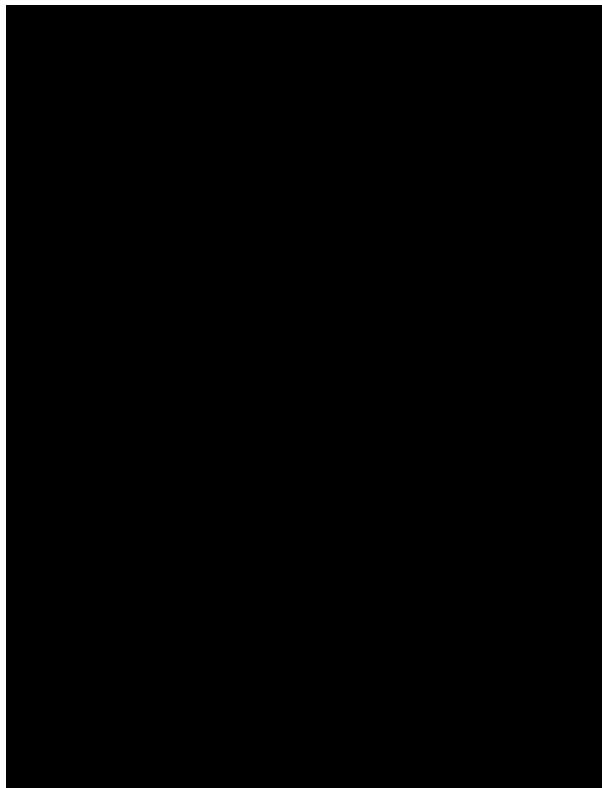
### **High-security Keys are Publicly Available**

High-security keys that allow access to the company's sensitive infrastructure and assets are available in the public domain, surfacing in online and brick-and-mortar marketplaces. [REDACTED]

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

[REDACTED] as Figure 5 illustrates.

**Figure 5.** [REDACTED]



Source: Screenshot of [REDACTED]

Note: Determining whether the company or another railroad issued these keys was outside the scope of our review.

We could not determine if any of these keys originated with current or former company employees because [REDACTED] keys could have also posted them for sale. Nonetheless, [REDACTED] indicates that the company is a known source. In addition, the company's Assistant Police Chief told us the company previously had [REDACTED]  
[REDACTED]  
[REDACTED]

Senior officials in the Service Delivery and Operations department and Corporate Security acknowledge that they cannot account for the keys the company has issued, and that this broad public availability of high-security keys presents security and safety

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

risks, potentially giving bad actors opportunities to disrupt train operations. Senior officials in the Service Delivery and Operations department told us the company has measures in place to mitigate some of the most serious risks. For example, officials told us the company's [REDACTED]<sup>8</sup> [REDACTED]

[REDACTED] In addition, senior Service Delivery and Operations officials told us that operating rules require train operators to act cautiously and to stop when they are uncertain, [REDACTED]

[REDACTED] Nonetheless, these officials noted [REDACTED] could disrupt operations and cause the company to incur unnecessary delays and costs.

## **Weak Controls Contribute to Availability of High-security Keys**

High-security keys are available in the public domain in part because the company does not have comprehensive controls over them. Industry standards suggest that organizations establish and implement policies, procedures, and control activities to minimize the possibility of unauthorized access to an entity's assets. Contrary to these standards,<sup>9</sup> however, the company does not consistently implement the following:

- marking keys with unique identifiers to distinguish one key from another
- using standardized forms for requesting or returning keys
- maintaining a list of high-security keys issued to personnel
- conducting periodic inventory reviews to determine if managers responsible for issuing keys are properly securing and accounting for them

Additionally, industry standards suggest that organizations adopt a corporate-wide policy on key management that assigns responsibilities for issuing, tracking, retrieving, and auditing keys. The company issues general guidance that instructs personnel to safeguard company-issued property, including keys, and directs them to return keys or other access devices in certain instances. It does not, however, have a comprehensive policy on managing, issuing, storing, retrieving, replacing, and accounting for all keys, or assigning responsibilities for doing so. In 2019, the company began drafting a policy

---

<sup>8</sup> [REDACTED]

<sup>9</sup> We reviewed practices recommended by global security device manufacturers and policies used by educational, government, and corporate entities who use high-security keys.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

to serve as a framework for controlling its high-security keys. As of September 2022, however, the company had not authorized or distributed the draft policy, and leadership from several affected departments told us they had not reviewed it. In addition, the draft policy incorporates industry-recommended activities—such as requiring departments to take specific actions regarding day-to-day management of keys—but it does not establish timelines for departments to implement them.

In the absence of a company-wide policy and controls, some divisions and supervisors responsible for issuing keys have made efforts to better track the keys they distribute. This provides some added security, but the controls we reviewed were ad hoc and inconsistent with industry standards; therefore, they likely do not materially reduce company risk. For example, the [REDACTED] group requires employees to sign a form when they receive an [REDACTED] key, but the group did not periodically review key distribution logs to verify their accuracy until June 2022. In another example, one IMCS supervisor developed a spreadsheet to track the location of [REDACTED] keys in his division. These keys, however, are generally not serialized and, in several instances, the division assigned keys to a vehicle or an entire work crew, making it difficult to enforce personal accountability.

The company has some requirements related to its high-security keys, but it is unclear how rigorously it enforces them. The Senior Director of Corporate Security told us the company considers all keys to be accountable property. In addition, the company's Employee Security Handbook requests that employees, vendors, and contractors return keys when they leave the company, complete contracted work, or transfer locations or departments. Multiple IMCS officials told us, however, that they personally attempt to retrieve keys when employees leave, but the company does not rigorously enforce requirements to return them. Moreover, one Material Control manager told us that employees do not turn them in when they transfer or leave the company, including when they are terminated.

Senior officials in the Service Delivery and Operations department and Corporate Security agreed that the company could implement stronger controls over its own keys, such as tracking to whom it issues new keys, which would help reduce the risk of unauthorized access over time. The company has not, however, formally identified and assessed the risks associated with high-security keys being available in the public domain or the practicality of mitigating those risks. This is particularly important because several factors could limit the extent to which the company can reduce this risk. Senior officials in the Service Delivery and Operations department told us it would be

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

futile to try to retrieve keys from employees who have left the company. In addition, some keys access [REDACTED]

[REDACTED] therefore, re-keying and replacing all these locks may not be cost-effective or practical. Furthermore, company officials told us [REDACTED]  
[REDACTED]  
[REDACTED]

In the face of these limitations, an assessment of the risks of high-security keys being available in the public domain and the practicality of implementing new controls could identify actions that are feasible. It would also help the company prioritize those actions that would provide a basis for stronger oversight. For example, Corporate Security officials agreed that re-keying all locks may not be practical, but identifying and documenting current keyholders might be.

### **Additional Controls Could Improve Company's Ability to Account for Its High-security Keys**

The company's recent distribution of Medeco® keys highlights the need for a company-wide policy that establishes controls over its high-security keys and assigns responsibilities. The company began distributing the Medeco® keys in April 2022 prior to having complete controls in place over their management, distribution, tracking, and retrieval.<sup>10</sup> The controls were not in place because Corporate Security and IMCS—the primary users of the Medeco® keys—disagreed on the role each should play in overseeing the keys. After the company started distributing Medeco® keys, IMCS designated four key control managers to be responsible for overseeing their general distribution and tracking, using sign-out forms and key inventory logs. The company also drafted a distribution plan that governs Medeco® key management in IMCS,<sup>11</sup> and Corporate Security and IMCS agreed to the draft plan in July 2022, which documents their responsibilities. In the interim, however, the company did not properly account for

---

<sup>10</sup> Medeco® keys are serialized consistent with industry practices, which supports tracking and retrieval.

<sup>11</sup> A Workforce Management official told us the group originally planned to finalize the draft in November 2022, but as of December 2022, it did not have an updated estimate for completion.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

the Medeco® keys and cannot account for at least 24 of the 3,500 Medeco® keys as of September 2022.

A company-wide policy that aligns with industry standards could minimize the risk of similar disagreements over responsibilities when the company issues high-security keys—Medeco® or otherwise—and improve the company’s ability to account for its keys. Although IMCS employees will be the primary users of the Medeco® keys, a Corporate Security official told us employees in the Capital Delivery department and Transportation group will also need them. Corporate Security expects these groups to develop and implement their own procedures in line with industry standards—similar to those developed by IMCS—or in line with the company-wide policy, once authorized and distributed. As of September 2022, however, they had not begun this process, and there is no requirement, such as a company-wide policy, for them to do so.

### **Centralized Key Management Could Help Company Control High-security Keys**

The company’s process for tracking its high-security keys is also ad hoc and siloed. Managers who track keys—such as the IMCS Medeco® key control managers and those in the Communications and Signals group—generally rely on paper-based forms and locally maintained spreadsheets. This occurs because the company does not have a centralized system or mechanism for tracking its high-security keys. Industry standards suggest that one option for doing so is to use software specifically designed for managing keys. Without such a centralized system, it is difficult for the company to track keys when employees change divisions, transfer to a new department, or move to a new geographic location. In addition, the current localized tracking tools used by managers make it difficult to determine which records are current and which are outdated, according to a senior IMCS official.

Corporate Security officials agreed that a centralized system that manages keys across the company would help track keys when employees change divisions or geographic locations. Further, the former Chief Operations Officer told us a company-wide, protected database could help the company better manage its high-security keys and reduce the risk of unauthorized access. According to this official, the company has not considered using such a database, but it could do so with support from the Digital Technology department.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

## CONCLUSIONS

Physical keys protect many of the company's [REDACTED] [REDACTED] Without rigorous controls, these keys can find their way into the hands of individuals who are not authorized to access these assets. Although some of these individuals may simply appreciate their novelty, it does not diminish the security risk posed because these keys access working locks that bad actors could use to disrupt the company's rail operations. [REDACTED]

[REDACTED] Nevertheless, developing robust policies, conducting regular oversight, and implementing stronger controls to the extent practical can minimize the risk that keys will find themselves in the hands of someone seeking to inflict harm against the company. Moreover, such steps are consistent with the company's goals of protecting its employees, passengers, and infrastructure.

## CONSIDERATIONS FOR MANAGEMENT

To further strengthen controls surrounding its high-security keys, the Chief Safety Officer, in consultation with the Executive Vice President, Service Delivery and Operations, may want to consider the following actions:

1. Develop and implement a company-wide key management policy that establishes control activities consistent with industry practices, assigns roles and responsibilities for these activities, and includes timelines for departments to comply with the provisions that require their action.
2. Identify and assess the relative risks associated with high-security keys in circulation and implement controls to mitigate them to the extent practical. Specifically, consider the following actions:
  - a. Conduct an inventory of current employees and contractors who hold high-security keys, including determining and documenting keyholders, their positions, and types of keys held.
  - b. Retrieve keys from current employees and contractors who no longer need them to execute regular work activities or who are preparing to leave the company.
  - c. Establish a process to regularly update the company's inventory of high-security keys.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

3. Establish a centralized system or mechanism for tracking high-security keys. One option could be to adopt key management software.

## **MANAGEMENT COMMENTS AND OIG ANALYSIS**

In commenting on a draft of this report, the Chief Safety Officer agreed with our considerations for management and described the company's plans to address them, which we summarize below.

**Consideration 1:** Management agreed with our consideration to develop and implement a company-wide key management policy. The company intends to issue a policy that establishes control activities consistent with industry practices, assigns roles and responsibilities, and sets appropriate timelines for departments to comply with the provisions that require their action. The target completion date is May 31, 2023.

**Consideration 2:** Management agreed with our consideration to implement controls that will mitigate the risks associated with high-security keys in circulation. Corporate Security seeks to implement an enterprise-wide inventory system for high-security keys to assist with their tracking and retrieval. In addition, Corporate Security will conduct periodic audits to ensure that departments comply with controls that the company will establish in its key management policy. The target completion date is September 30, 2024.

**Consideration 3:** Management agreed with our consideration to establish a centralized system to track high-security keys. Corporate Security plans to work with other departments to develop a centralized system and processes to track high security keys. The target completion date is September 30, 2024.

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

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

## APPENDIX A

### **Objective, Scope, and Methodology**

This management advisory report provides the results of our review of the company's controls over its high-security keys. Our objective was to assess the extent to which the company has controls to manage, distribute, track, and retrieve high-security keys. Our scope focused on high-security keys that company employees use, including [REDACTED]

[REDACTED] We performed our work from March 2022 to October 2022 in [REDACTED] Providence, Rhode Island; [REDACTED] [REDACTED] and Washington, D.C. Certain information in this report has been redacted due to its sensitive nature.

To identify industry practices that would serve as criteria to assess the company's controls, we reviewed control practices recommended by global security device manufacturers, and we reviewed policies used by educational, government, and corporate entities who use high-security keys.

To determine the extent to which the company had controls over its high-security keys, we reviewed company procedures, processes, and draft policies regarding key management. We also interviewed officials in the Service Delivery and Operations; Capital Delivery; and Safety, Health, and Environmental departments to understand existing controls over high-security keys and the risks associated with an absence of controls. We then compared the company's practices to industry standards to determine gaps in controls.

We conducted site visits in [REDACTED] to observe the [REDACTED] [REDACTED] We also observed the Medeco® keys in use and [REDACTED]  
[REDACTED]

We conducted our work in accordance with standards we developed for alternative products.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
 over High-security Keys**  
 OIG-MAR-2023-003, December 12, 2022

**APPENDIX B**  
**Management Comments**

NATIONAL RAILROAD PASSENGER CORPORATION

**Memo**



*SM*

Date	November 18, 2022	From	Steven Predmore, EVP CSO
To	Jim Morrison, Assistant Inspector General, Audits	Department	Operations
		cc	Stephen Gardner, CEO Roger Harris, President Eleanor Acheson, EVP General Counsel John Carroll, Sr. Director Corporate Security Sam Dotson, VP Corp Security & Chief of Police Laura Mason, EVP Major Program Delivery Dennis Newman, EVP Strategy & Planning Qiana Spain, EVP CHRO Gerhard Williams, EVP Service Delivery & Operations Tracie Winbigler, EVP CFO Christian Zacariassen, EVP Digital Technology & Innovation Mark Richards, Sr. Director Amtrak Risk & Controls
Subject: Management Response to PHYSICAL SECURITY: Amtrak has Opportunities to Strengthen Controls over High-security Keys ( <i>Draft Management Advisory Report for Project No. 012-2022</i> )			

This memorandum provides Amtrak's response to the draft management advisory report titled, "Amtrak has Opportunities to Strengthen Controls over High-security Keys." Management appreciates the opportunity to respond to the OIG's considerations for management (observations). The observations provided meaningful input and we have provided management responses below:

**Observation 1:**

Develop and implement a company-wide key management policy that establishes control activities consistent with industry practices, assigns roles and responsibilities for these activities, and includes timelines for departments to comply with the provisions that require their action.

**Management Response/Action Plan:**

Amtrak Corporate Security (CS) commits to issuing a company-wide key control management policy that establishes control activities consistent with industry best practices. This policy assigns roles and responsibilities to those activities specified in the policy. CS will also work with other business units to set appropriate timelines.

**Responsible Amtrak Official(s):** John Carroll, Sr. Director Corporate Security  
 Gerhard Williams, EVP SD&O

**Target Completion Date:** May 31<sup>st</sup>, 2023.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

NATIONAL RAILROAD PASSENGER CORPORATION

**Observation 2:**

Identify and assess the relative risks associated with high-security keys in circulation and implement controls to mitigate them to the extent practical. Specifically, consider the following actions:

- a. Conduct an inventory of current employees and contractors who hold high-security keys, including determining and documenting keyholders, their positions, and types of keys held.
- b. Retrieve keys from current employees and contractors who no longer need them to execute regular work activities or who are preparing to leave the company.
- c. Establish a process to regularly update the company's inventory of high-security keys.

**Management Response/Action Plan:**

Corporate Security (CS) agrees that there are risks associated with the high-security keys in circulation. CS seeks to implement controls that will mitigate these risks to the extent practical.

- a. As the OIG acknowledged in the report, it would be extremely challenging to retrieve all high-security keys from current and former Amtrak employees, contractors, and other railroad personnel. CS, in conjunction with other business units, will seek to implement an enterprise wide high-security key inventory system to allow Amtrak business units to track their key inventory and reduce risks associated with high-security keys in circulation.
- b. Amtrak's revised key control policy states that the key control manager is responsible for the return of keys when the key holder's responsibilities have changed, and access is no longer needed. The high-security key inventory system will assist the key control manager with the tracking and retrieval of keys.
- c. Amtrak's revised key control policy states that the key control manager is responsible for updating their inventory of high-security keys. CS can assist the key control managers with the development of their processes and procedures. CS will conduct periodic audits of the high-security key inventory to ensure compliance with these controls.

**Responsible Amtrak Official(s):** John Carroll, Sr. Director Corporate Security  
Gerhard Williams, EVP SD&O

**Target Completion Date:** September 30<sup>th</sup>, 2024.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

NATIONAL RAILROAD PASSENGER CORPORATION

**Observation 3:**

Establish a centralized system or mechanism for tracking high-security keys (One option would be to adopt key management software).

**Management Response/Action Plan:**

CS commits to work with the other business units to develop a centralized key management system, and processes to track high security keys.

**Responsible Amtrak Official(s):** John Carroll, Sr. Director Corporate Security  
Gerhard Williams, EVP SD&O

**Target Completion Date:** September 30<sup>th</sup>, 2024.

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

## APPENDIX C

### Abbreviations

IMCS	Infrastructure Maintenance and Construction Services
[REDACTED]	[REDACTED]
OIG	Amtrak Office of Inspector General
the company	Amtrak

*Amtrak Office of Inspector General*  
**Safety and Security: Amtrak Has Opportunities to Strengthen Controls  
over High-security Keys**  
OIG-MAR-2023-003, December 12, 2022

## **APPENDIX D**

### **OIG Team Members**

Leila Kahn, Senior Director

Todd Kowalski, Senior Audit Manager

Sarah Brandes, Senior Auditor

Richard Weiland, Senior Auditor

Alison O'Neill, Communications Analyst

## **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](http://www.amtrakoig.gov)

**Reporting Fraud, Waste, and Abuse**  
Report suspicious or illegal activities to the OIG Hotline  
[www.amtrakoig.gov/hotline](http://www.amtrakoig.gov/hotline)  
or  
800-468-5469

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