New report: Amtrak has opportunities to strengthen controls over high-security keys

For Immediate Release
December 14, 2022

WASHINGTON – Amtrak has not consistently implemented controls over the distribution, tracking, and retrieval of its high-security keys, which contributes to security and safety risks, an Amtrak Office of Inspector General report released today said.

According to the report, high-security keys are physical keys used by Amtrak employees and contractors to access critical and sensitive infrastructure. In July 2022, an OIG investigation found that a Florida-based employee attempted to sell high-security keys online, which prompted this most recent review. The employee was charged by the state of Florida on November 28, 2022, for attempting to sell the keys and for dealing in stolen property, according to court records.

Such high-security keys are broadly available to the public and can surface in online and brick-and-mortar marketplaces, contributing to security and safety risks, the report said. Senior officials told the OIG that Amtrak has measures in place to largely mitigate serious risks, but the availability of these keys could still give bad actors an opportunity to disrupt train operations, causing unnecessary delays and costs.

The report notes that Amtrak's high-security keys are available in the public domain in part because the company does not have comprehensive controls over them. Amtrak officials told the OIG that, although they could not account for all the keys the company has issued, it would be futile to try to retrieve them from former employees and that rekeying and replacing locks in use across Amtrak's infrastructure would be cost-prohibitive.

In the absence of a company-wide policy and controls, some divisions and supervisors responsible for issuing keys have made efforts to better track high-security keys. These efforts provide extra security, but are *ad hoc* and inconsistent with industry standards and likely do not materially reduce company risk, the report said. While Amtrak has stated in its Employee Security Handbook that employees, vendors, and contractors should return keys when they leave the company, complete contracted work, or transfer to another location, the company does not rigorously communicate about or enforce these requirements.

The report offered several considerations for Amtrak to help address the OIG's observations. They include 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, Amtrak may want to consider developing a key management policy that institutes new controls and establishing a centralized mechanism for tracking high-security keys, such as key management software, the report said.

More information is included in the full report which can be downloaded on the OIG's website: https://direc.to/iwkA.

-###-