OFFICE OF INSPECTOR GENERAL

Audit Report

Report on Cybersecurity Information For Covered Systems at the Railroad Retirement Board

This abstract summarizes the results of the subject audit. The full report includes information protected from disclosure and has been designated for limited distribution pursuant to 5 U.S.C. § 552

Report No. 16-09
August 10, 2016

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Report on Cybersecurity Information For Covered Systems at the Railroad Retirement Board

This report presents the results of the Office of Inspector General's (OIG) review of cybersecurity information for covered systems in accordance with the Consolidated Appropriations Act of 2016, Public Law 114-113. The OIG is required to obtain and report information from the Railroad Retirement Board (RRB) about specific information in the agency's covered Federal computer systems that provide access to personally identifiable information.

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and Railroad Unemployment Insurance Act. The programs provide income protection during retirement and in the event of disability, death, temporary unemployment, or sickness. To accomplish its benefit payment mission, the RRB uses many agency operated component applications and some contractor operated systems/services, all with access to personally identifiable information and considered a covered Federal computer system.

Objective

The objective of this review was to prepare a report on the agency's cybersecurity program as mandated in the Consolidated Appropriations Act of 2016. Specifically, this included information on the RRB's logical access controls, RRB multi-factor authentication for privileged users, software inventories and licenses for the RRB and its contractors, and threat monitoring and detection capabilities for the RRB and its contractors. We have also included information on the assurance information the RRB obtains for its contractors. Unless required to do so, this report did not assess the efficacy of the cybersecurity program at the RRB.

Results of Review

The RRB has established logical access control policies and procedures to guard against unauthorized access and enforce least privilege. Past OIG reviews of the RRB's identity and access management program show that it is consistent with applicable standards, but some improvement is necessary to be fully effective.

Multi-factor authentication has not been established for privileged users due to issues that arose from the use of multiple accounts for these users. The RRB understands the requirement for using multi-factor authentication for privileged accounts and has developed a project plan to implement a solution.

The RRB and its contractors have established configuration management policies and procedures that include developing, documenting, and keeping current an inventory of software and associated license information. The inventories are periodically reviewed and updated as appropriate.

The RRB and its contractors have established capabilities to monitor and detect exfiltration and other threats, including data loss prevention, forensics and visibility, and digital rights management.

The RRB obtains security assurances from their contractors that either operate an interconnected external system or when the contractor stores RRB data on their contractor information system. Other contractors, such as those used for staff augmentation, are required to participate in the RRB's security and privacy training program. Past OIG audits show that the RRB's information security program associated with contractor operations or services requires improvement.