OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2014 Audit of Information Security 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

This abstract was revised on April 16, 2015, to correct a typographical error in the Results of Audit section. This correction had no impact on the conclusions presented, and the underlying restricted distribution audit report required no change.

Report No. 15-04
March 16, 2015

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2014 Audit of Information Security at the Railroad Retirement Board

The Office of Inspector General for the Railroad Retirement Board (RRB) conducted an audit of information security at the RRB for fiscal year 2014, which is mandated by the Federal Information Security Management Act of 2002 (FISMA).

Objectives

The objectives of our audit included testing the effectiveness of the information security policies, procedures, and practices of a representative subset of the agency's information systems; assessing agency compliance with FISMA requirements and related information security policies, procedures, standards and guidelines; and preparing a report on selected elements of the agency's information security program in compliance with the Office of Budget and Management fiscal year 2014 FISMA reporting instructions.

Results of Audit

Our audit determined that the RRB continues to make progress in implementing an information security program that meets the requirements of FISMA; yet a fully effective security program has not been achieved. In fiscal year 2014, the RRB strengthened controls in their risk management and continuous monitoring program to mitigate the significant deficiencies in the internal control structure over the review of the agency's contractor deliverables associated with the risk management framework and the security configuration management program. However, we noted some lesser deficiencies in the RRB's security program.

Recommendations

In total, we made nine detailed recommendations to RRB management related to:

- Strengthening Risk Management and Continuous Monitoring Management by developing and implementing a continuous monitoring strategy and risk assessment that is compliant with federal guidelines and provides ongoing information security continuous monitoring.

- Improving the configuration management process by developing procedures to ensure all devices are included in the regularly scheduled vulnerability and compliance scans, all servers are regularly patched to remediate vulnerabilities, and adequate staff support exists for workstation patching.

- Strengthening Identity and Access Management by developing operating procedures for security access systems, including data entry and document retention, and removing user accounts from the all security systems upon separation from the agency.

- Revising procedures relating to Incident Response and Reporting to comply with new federal guidelines, as well as ensuring potential personally identifiable information breaches are fully documented and retained in agency records.

- Improving the contractor systems process by identifying all systems and services provided by external entities and implementing controls to ensure all contractors are compliant with FISMA requirements.

Management's Responses

Agency management concurs with all recommendations.