OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2015 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

Report No. 16-06
April 26, 2016

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2015 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 2015, as mandated by the Federal Information Security Modernization Act of 2014 (FISMA). This Act modified the Federal Information Security Management Act of 2002 and included changes in the requirements for evaluations performed by Inspectors General. FISMA now requires an assessment of effectiveness of the agency's information security policies, procedures, and practices, rather than an assessment of compliance. An assessment of effectiveness considers internal control integration and whether the organization is achieving its intended objective.

Objectives

The objectives of our audit included:

- testing the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;
- assessing the effectiveness of the information security policies, procedures, and practices of the agency; and
- preparing a report on selected elements of the agency's information security program in compliance with the fiscal year 2015 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. Our audit identified deficiencies in the areas of continuous monitoring management, configuration management, identity and access management, remote access management, incident response and reporting, plan of action and milestones, and security training.

Recommendations

In total, we made 23 detailed recommendations to RRB management related to assorted policies, procedures, and time standards; exploring new automated technology products; access control; training; updating agency records; and implementing stronger controls.

Management's Responses

Agency management concurs will all recommendations.