OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2013 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. 14-03
March 04, 2014

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2013 Audit of Information Security at the Railroad Retirement Board

Background

The Office of Inspector General for the Railroad Retirement Board (RRB) conducted an audit of information security at the RRB for fiscal year (FY) 2013, 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 Department of Homeland Security's FY 2013 FISMA reporting instructions.

Findings

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. 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 remain unresolved. We also noted some lesser deficiencies in the RRB's security program.

Recommendations

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

- Strengthening Configuration Management by developing baseline configuration settings and implementing automated capabilities to identify deviations from baseline configurations settings.
- Ensuring non-user accounts are reviewed periodically including updating the accounts as necessary to ensure account names and descriptions accurately reflect the purpose of the account.
- Identifying all key data fields for effective management in the agency-wide Plan of Action and Milestones, and strengthening controls to ensure all key fields are required data fields and consistently completed.

- Improving the security training process by implementing controls to ensure all contractors complete security awareness training.
- Updating policies and procedures for role-based training for RRB employees and contractors.

Management's Responses

Agency management concurs with all recommendations.