OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2012 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. 13-04
February 12, 2013

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2012 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 (FY) 2012, which is mandated by the Federal Information Security Management Act of 2002 (FISMA). 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; and preparing a report on selected elements of the agency's information security program in compliance with the Department of Homeland Security's FY 2012 FISMA reporting instructions.

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. In total, we made 19 detailed recommendations to RRB management related to:

- Ensuring compliance with recommended system configuration requirements, including documenting all necessary deviations and adherence to change control procedures for maintaining testing and approval documentation.
- Strengthening Identity and Access Management by revising procedures to allow for the extension of equipment and account privileges based only on written documentation, and the retention of that documentation.
- Revising procedures relating to Incident Response and Reporting in order to reduce delays in reporting potential personally identifiable information breaches.
- Improving remediation of security weaknesses by developing time standards and controls for entering weaknesses and ensuring all data fields are completed in the agency-wide Plan of Action and Milestones, as well as providing access and training to new users.
- Participation of all system owners in disaster recovery testing, comprehensive updates to the Business Impact Analysis and Business Continuity Plan documents, and the development of system specific contingency plans which show the test coverage and frequency.
- Updating appropriate processes and procedures for security awareness training required for RRB employees and contractors.

Agency Management has agreed to take corrective actions for all recommendations.