OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2011 Evaluation 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. 12-02
January 05, 2012

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Fiscal Year 2011 Evaluation of Information Security at the Railroad Retirement Board

The Office of Inspector General for the Railroad Retirement Board (RRB) conducted an evaluation of information security at the RRB for fiscal year (FY) 2011, which is mandated by the Federal Information Security Management Act of 2002 (FISMA). The objectives of our evaluation included testing the effectiveness of the information security policies, procedures, and practices of a representative subset of the agency's information systems; and a report on selected elements of the agency's information security program to be prepared in compliance with Office of Management and Budget's FY 2011 FISMA reporting instructions.

In a separately issued Restricted Distribution report, we communicated 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 deficiency in the internal control structure over the review of contractor deliverables, associated with the risk management framework, remains unresolved. Additionally, we are citing the RRB with a significant deficiency in its security configuration management program. We also noted some lesser deficiencies in the RRB's security program. In total, we made 13 detailed recommendations to RRB management related to:

- developing and implementing a comprehensive risk management governance strategy that builds information security capabilities into federal information systems, maintains awareness of the systems' security state, and provides essential information to facilitate decisions;
- obtaining the necessary funding and resources to decommission unsupported equipment;
- providing additional security awareness training to employees;
- improving data collection methods, and performing a quality assurance review of security incidents and data reported internally and externally;
- implementing and performing a quarterly quality assurance review for the preparation and processing of system access re-authorizations; and
- formally reviewing and publishing the agency's Capital Planning and Investment Control Guide.

RRB management has agreed to take corrective actions for all recommendations.