OFFICE OF INSPECTOR GENERAL

Audit Report

Inspection of the Railroad Retirement Board's Financial Interchange System Continuous Monitoring

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. 12-08
September 21, 2012

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Inspection of the Railroad Retirement Board's Financial Interchange System Continuous Monitoring

The Office of Inspector General (OIG) for the Railroad Retirement Board (RRB) conducted an inspection of the activities at the RRB for the continuous monitoring of the Financial Interchange (FI) system to determine adherence with existing policy, procedures, guidance, and standards. Because the FI system inherits many of its controls from the Agency Enterprise General Information Support System (AEGIS) this inspection also includes an evaluation of the continuous monitoring documentation prepared for the AEGIS system. This inspection will support the OIG's mandated fiscal year (FY) 2012 Federal Information Security Management Act of 2002 evaluation.

The objective of continuous monitoring is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time. Continuous monitoring is an important activity in assessing the security impact on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation. In FY 2011, a contractor was hired by the RRB to plan and perform continuous monitoring of the controls over the RRB's FI and AEGIS systems.

Our evaluation determined that activities conducted at the RRB for the continuous monitoring process of the FI and AEGIS systems do not fully comply with existing policy, procedures, guidance, and standards because evidence suggests that an ineffective review process was performed over contractor deliverables. Therefore, we will continue to cite the agency with a significant deficiency in the internal control structure over the review of contractor deliverables associated with the risk management framework. We made eleven detailed recommendations to RRB management related to:

- improving the controls over the review process for the continuous monitoring deliverables received from the contractor and approved by the RRB;
- allocating the necessary resources to allow for an effective review of the continuous monitoring documentation; and
- effectively managing and consistently updating the FI and agency-wide Plan of Action and Milestones.

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