OFFICE OF INSPECTOR GENERAL

Audit Report

Inspection of the Railroad Retirement Board's Agency Enterprise General Information Support System Certification and Accreditation

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. 11-10
September 28, 2011

RAILROAD RETIREMENT BOARD

REPORT ABSTRACT
Inspection of the Railroad Retirement Board's Agency Enterprise General Information Support System Certification and Accreditation

The Office of Inspector General (OIG) of the Railroad Retirement Board (RRB) conducted an inspection to determine whether the activities conducted at the RRB for the certification and accreditation of the Agency Enterprise General Information Support System (AEGIS) comply with existing policy, procedures, guidance, and standards.

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to establish and maintain an agency wide security management program that includes testing of security controls with a frequency that is no less than annually. In addition to testing security controls, an agency official must authorize the system for processing. This authorization must be in writing and must occur at least every three years. In fiscal year (FY) 2010, RRB hired a contractor to conduct a certification and accreditation, currently referred to as a system authorization, for AEGIS.

In a separately issued Restricted Distribution report, we communicated that the activities conducted at RRB for the certification and accreditation do not fully comply with existing policy, procedures, guidance, and standards. In our FY 2009 FISMA report, the OIG cited the RRB with a significant deficiency in internal control over the certification and accreditation process because of an ineffective review process for contractor deliverables. Our inspection found that the internal control structure over the certification and accreditation process is still a significant deficiency. We made three recommendations to RRB management:

- to develop a comprehensive review process that includes a comparison of the documents for consistency and verification that all of the requirements for applicable controls are adequately addressed;
- to review prior plan of action and milestones (POAM) items and update the current agency wide POAM to include all outstanding weaknesses for the AEGIS system; and
- to develop and implement detailed POAM procedures for maintaining the information necessary to allow independent verification and validation of POAM closures, and for tracking of agency corrective action by the Chief Information Officer.

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