OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2010 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. 11-01
November 05, 2010

RAILROAD RETIREMENT BOARD

Report Abstract
Fiscal Year 2010 Evaluation of Information Security At the Railroad Retirement Board

This abstract summarizes the results of the Office of Inspector General (OIG) evaluation of Information Security for the Railroad Retirement Board (RRB) for FY 2010.

The Federal Information Security Management Act of 2002 (FISMA) mandates that agencies develop, document and implement an agency wide information security program. FISMA establishes minimum requirements for the management of information security.

The RRB's information system environment consists of three major application systems and one general support system, each of which has been designated as a moderate impact system in accordance with standards and guidance promulgated by the National Institute of Standards and Technology (NIST).

The RRB has made significant progress in implementing an information security program that meets the requirements of FISMA; yet a fully effective program has not been achieved. For example, the RRB has taken action to address their significant deficiency in access controls; but a significant deficiency remains in internal control over the certification and accreditation review process of contractor deliverables.

During FY 2010, we observed that the RRB's program for ensuring agency servers comply with required configuration settings is not fully effective, and the agency did not complete external reports of all Category 1 security incidents. Previously identified weaknesses in the areas of security plans, information security and privacy training, periodic testing and evaluation, an effective remedial action process, continuity of operations, the inventory of systems, risk assessment, and privacy continue to exist. Also, although the agency addressed the significant deficiency in access controls, weaknesses in that area still need to be addressed.

The RRB continues to address open audit recommendations pertaining to their information security weaknesses.

Certification and Accreditation

The RRB's certification and accreditation program remains ineffective because of a significant deficiency in the internal control structure over the review of contractor deliverables. We found that actions taken to date would not allow for accurate and reliable information consistently among individual reviewing offices over time. As a result, the RRB cannot ensure that the information systems are operating at an acceptable level of risk to agency operations, assets, or individuals. Since final documentation supporting the results of the contractor's work is not expected to be completed until early FY 2011, we were unable to fully assess this area of the RRB's information security program.

Policies and Procedures

The RRB continues to need improvement in implementing risk-based policies and procedures that are comprehensive and effective in all areas of the agency's information security and privacy programs. In FY 2010, the agency began conducting routine vulnerability scans, but does not have a procedure to consider all relevant factors when determining which vulnerabilities to remediate. We also observed that the agency was not performing routine scans to ensure compliance with the agency wide configuration policy settings. Risk-based policy and procedures serve to secure the agency's information and information systems. Compliance scans for server settings alert the agency where modifications need to be made to ensure a more secure environment.

Incident Handling and Reporting

The RRB's incident handling and reporting program is generally effective in ensuring the confidentiality, integrity, and availability of the agency's information and information technology; however, we found that some incidents were not reported externally to the United States Computer Emergency Readiness Team (US-CERT) as required. Because the RRB misapplied OMB criteria for external breach notification, they failed to report incidents of potential PII breaches to US-CERT. As a result, they are not in full compliance with incident handling and reporting requirements.

We have made specific recommendations for corrective actions to address the weaknesses identified in our audit. The Bureau of Information Services has agreed to implement our recommendations to improve the information security program at the RRB.