U.S. RAILROAD RETIREMENT BOARD

OFFICE OF INSPECTOR GENERAL

This report summary presents the abbreviated 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.

Fiscal Year 2017 Audit of Information Security at the Railroad Retirement Board

Report No. 18-06

June 5, 2018

OFFICE OF INSPECTOR GENERAL
U.S. RAILROAD RETIREMENT BOARD
Fiscal Year 2017 Audit of Information Security At the Railroad Retirement Board

What We Found

Our audit determined that RRB continues to make progress in implementing an information security program that meets the requirements of FISMA; yet RRB's efforts continue to be ineffective due to the numerous open audit recommendations related to strategy plans, policies and procedures, resource allocation, and performance metrics. Implementation of these audit recommendations would allow RRB to meet requirements to achieve higher levels of maturity established in the maturity model developed by the Office of Management and Budget and the Department of Homeland Security. We found that each of the seven OIG FISMA metric domains and the corresponding cybersecurity framework functions were assessed as "Not Effective" when evaluated using the maturity model.

The overall information security program has weaknesses that impact more than one area of the cybersecurity framework. These weaknesses include a growing number of aging weaknesses on RRB's Plan of Action and Milestones, continued problems with maintaining current and comprehensive policy and procedures, and current gaps in RRB's privacy program. Our review also identified deficiencies in the areas of risk management, configuration management, identity and access management, incident response, and contingency planning.

What We Recommend

To address the weaknesses identified in this audit, we made 21 detailed recommendations related to improving the information security program at RRB. These recommendations would improve policies, procedures, and plans; resource management; performance management; agency records; technologies to improve incident response; disaster recovery testing; and strengthen controls.

RRB management concurred with 20 recommendations, and partially concurred with 1 recommendation.

What We Did

The Office of Inspector General (OIG) for the Railroad Retirement Board (RRB) conducted an audit of information security at RRB for fiscal year 2017. This audit was mandated by the Federal Information Security Act of 2014 (FISMA).

Our objectives were to test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; conduct an assessment of the effectiveness of RRB's information security policies, procedures, and practices; and report on the selected elements of the agency's information security program prepared in compliance with the fiscal year 2017 FISMA reporting instructions.

The scope of this evaluation is information security at the RRB during fiscal year 2017.

We assessed the effectiveness of the information security program using the OIG FISMA metrics developed by the Office of Management and Budget and Department of Homeland Security.