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.

Performance Audit of RRB's Compliance with the Federal Information Security Modernization Act of 2014 Fiscal Year 2018

Report No. 19-03

December 19, 2018

OFFICE OF INSPECTOR GENERAL
U.S. RAILROAD RETIREMENT BOARD

Performance Audit of RRB's Compliance with the Federal Information Security Modernization Act of 2014 Fiscal Year 2018

What Kearney Found

"Kearney determined that RRB did not comply with FISMA legislation and [Office of Management and Budget] OMB guidance and that sampled security controls selected from [National Institute of Standards and Technology Special Publication] NIST SP 800-53, Rev.4 demonstrated ineffectiveness, and thus the RRB's Information Security Program did not provide reasonable assurance of adequate security." Each of the eight Federal Information Security Act of 2014 (FISMA) metric domains and their corresponding cybersecurity framework functions were assessed as "Not Effective" when evaluated using the maturity model. However, Kearney found that the RRB has established an Information Security Program and practices, and has implemented controls to support the Cybersecurity framework. Additional work is needed to achieve a rating of effective because of shortfalls in select information technology (IT) security controls. Kearney issued 31 recommendations in FISMA domain areas.

The overall information security program has weaknesses that impact the cybersecurity framework. These weaknesses include deficiencies in the areas of risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response, and contingency planning.

What Kearney Recommends

To address the weaknesses identified in this audit, Kearney made 31 detailed recommendations. RRB Management concurred with 30 of the recommendations. Kearney stated that implementing "the recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of RRB sensitive, non-public information; improve compliance with FISMA requirements; and assist the RRB Information Security Program reach the next maturity level."

RRB management disagreed with the conclusion that the RRB Information Security Program is not providing adequate assurance of adequate security.

What We Did

The Office of Inspector General (OIG) for the Railroad Retirement Board (RRB) engaged Kearney & Company, P.C. (Kearney) to conduct a performance audit of information security program at RRB for fiscal year 2018. This audit, which was conducted in accordance with the performance audit standards established by Generally Accepted Government Auditing Standards (GAGAS), was mandated by the Federal Information Security Act of 2014 (FISMA). Kearney is responsible for the audit report and the conclusions expressed therein. RRB OIG does not express any assurance on the conclusions presented in Kearney's audit report.

The scope of this audit is information security at the RRB during fiscal year 2018.