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 for Fiscal Year 2020

Report No. 21-03

January 14, 2021

OFFICE OF INSPECTOR GENERAL
U.S. RAILROAD RETIREMENT BOARD

Performance Audit of RRB's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020

What Kearney Found

"…Kearney determined that RRB did not comply with the [Federal Information Security Modernization Act of 2014] FISMA legislation and [Office of Management and Budget] OMB guidance and that sampled security controls selected from [National Institute of Science and Technology Special Publication] NIST SP 800-53, Rev. 4 demonstrated ineffectiveness; thus, RRB's Information Security Program [ISP] did not provide reasonable assurance of adequate security." Kearney noted that RRB's ISP did not meet the fiscal year 2020 Inspector General (IG) FISMA Reporting Metrics' definition of "effective" because the program's overall maturity did not reach Level 4: Managed and Measurable.

During fiscal year 2020, Kearney determined that policies and procedures are not regularly updated and have not been developed for a number of systems and controls, and standard operating procedures had not been developed for a majority of the tools procured to improve incident response.

Based on Kearney's audit work and the instructions in fiscal year 2020 IG FISMA Reporting Metrics, they concluded that RRB's ISP was not operating effectively.

What Kearney Recommends

To address the weaknesses identified in this audit, Kearney made 12 detailed recommendations. RRB management concurred with all of the recommendations. Kearney stated that "[i]mplementing our 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 ISP reach the next maturity level."

Kearney's review of RRB's management's response noted the recognition of necessary improvements to mature RRB's ISP and defined the Chief Information Officer and Chief Information Security Officer's planned actions to address the findings and recommendations presented in the report.

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 the ISP at RRB for fiscal year 2020. This audit, which was conducted in accordance with the performance audit standards established by Generally Accepted Government Auditing Standards, was mandated by 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 2020.

The objectives of this performance audit were to evaluate the effect of the RRB's ISP and practices and respond to the Department of Homeland Security's *Fiscal Year 2020 Inspector General FISMA Reporting Metrics,* dated April 17, 2020.