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 2022

Report No. 23-02

January 18, 2023

# *Performance Audit of RRB's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022*

## What Kearney Found

Kearney & Company, P.C. (Kearney) determined that Railroad Retirement Board (RRB) did not comply with Federal Information Security Modernization Act of 2014 (FISMA) legislation and Office of Management and Budget guidance and that sampled security controls selected from National Institute of Science and Technology Special Publication 800-53, Rev. 5 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 2022 Core Inspector General FISMA Reporting Metrics' definition of effective because the program's overall maturity did not reach Level 4: *Managed and Measurable*. Kearney noted various improvements across the agency that demonstrated RRB's commitment towards progress and noted that RRB has ongoing initiatives that, if fully implemented, will further mature RRB's ISP and practices.

Based on Kearney's audit work and the instructions in fiscal year 2022 Core Inspector General 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 11 recommendations. RRB management concurred with all of the recommendations. Implementing Kearney's recommended corrective actions will help minimize the risk of unauthorized disclosure, modification, use, and disruption of RRB's sensitive, non-public information, improve compliance with FISMA requirements, and assist the RRB ISP reach the next maturity level.

Kearney's review of RRB 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

RRB Office of Inspector General (OIG) engaged Kearney to conduct a performance audit of the ISP at RRB for fiscal year 2022. 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 the audit was information security at the RRB during fiscal year 2022. The audit team's period of performance to conduct the RRB FISMA audit was from March 1, 2022 through December 31, 2022.

The objectives of this performance audit were to evaluate the effectiveness of the RRB's ISP and practices, including RRB's compliance with FISMA, as well as any related information security policies, procedures, standards, and guidelines. This engagement also included a written response that addressed the Department of Homeland Security's *Fiscal Year 2022 Core Inspector General (IG) FISMA Reporting Metrics*.