



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.*

# Audit of the Railroad Retirement Board's Compliance with the FISMA of 2014 for Fiscal Year 2023

Report No. 24-05

April 10, 2024



## **What Castro Found**

For fiscal year 2023, Castro and Company, LLC. (Castro) determined that the Railroad Retirement Board (RRB) has sustained or continued to improve the Core Federal Information Security Modernization Act of 2014 (FISMA) Inspector General (IG) metrics reviewed in this audit. Although the RRB continued to improve its information security program (ISP), the majority of cybersecurity framework functions were rated below Managed and Measurable (Level 4), which is how the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) define an effective information security program. As a result, Castro concluded the RRB's ISP was not effective.

Due to the sensitivity of this report, the causes for majority of RRB's cybersecurity framework functions rated below Managed and Measurable (Level 4) can be found in the full audit report.

## **What Castro Recommended**

To address the issues identified in this audit, Castro made 13 recommendations. RRB management concurred with all 13 recommendations. Implementing Castro's recommended corrective actions will help minimize the risk of unauthorized access, disclosure, and use of RRB's sensitive non-public information, improve compliance with FISMA requirements, and assist the RRB's ISP to reach the next maturity level.

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's Office of Inspector General (OIG) engaged Castro to conduct a performance audit of the RRB's ISP for fiscal year 2023. This audit was conducted in accordance with generally accepted government auditing standards and was mandated by FISMA. Castro is responsible for the audit report and the conclusions expressed therein. RRB OIG does not express any assurance on the conclusions presented in Castro's audit report.

The scope of the audit was the RRB's ISP for fiscal year 2023. Castro evaluated one of the five major information systems of the RRB. The audit team performed this audit from July 2023 through January 2024.

The objectives of this performance audit were to evaluate the effectiveness of the RRB's ISP and policies, procedures, practices, standards, and guidelines, including RRB's compliance with FISMA. Castro also prepared responses to the annual IG FISMA reporting metrics, which the RRB's OIG submitted via DHS's CyberScope application.