



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 2026

Report No. 26-09

September 29, 2026

OFFICE OF INSPECTOR GENERAL U.S. RAILROAD RETIREMENT BOARD

Audit of the RRB's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal year 2026



What Castro Found

For fiscal year 2026, Castro and Company, LLC (Castro) determined that the Railroad Retirement Board (RRB) has largely sustained its maturity levels for the Core Federal Information Security Modernization Act of 2014 (FISMA) Inspector General (IG) metrics reviewed in this audit, even with decreases observed in three metrics. Castro did not identify any new findings during this audit because the prior-year findings were reported in prior-year FISMA audit reports and remain uncorrected. While the RRB generally sustained its information security program (ISP), all its cybersecurity framework functions were rated below "Managed and Measurable" (Level 4). The Office of Management and Budget, Department of Homeland Security (DHS), and the Council of the Inspectors General on Integrity and Efficiency define that as ineffective. As such, Castro concluded that the RRB's ISP was "not effective".

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

What Castro Recommended

Castro did not issue any new recommendation due to several prior-year recommendations remaining open. Implementing the prior-year recommendations that directly impact the RRB's ISP, which if effectively addressed, would strengthen the RRB's overall FISMA program maturity.

RRB management's response noted the recognition of the necessary improvements needed to mature the RRB's ISP and cited that additional funding and additional staffing is needed for a variety of reasons.

What We Did

RRB Office of Inspector General (OIG) engaged Castro to conduct a performance audit of the RRB's ISP for fiscal year 2026. Castro conducted this audit 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 2026. Castro evaluated five out of five RRB's major information systems. The audit team performed this audit from February 12, 2026 through July 7, 2026.

The objectives of this performance audit were to evaluate the effectiveness of the RRB's ISP and its 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.