Report Highlights

Federal Reserve: Security Control Review of Select Information Systems

Why This Matters

The Board of Governors of the Federal Reserve System maintains sensitive economic and financial data. A cybersecurity breach or compromise of the Board's systems could expose confidential supervisory information or personal information, impair banking oversight, or disrupt technical work related to currency.

Key Results

The Board's security control environment has targeted opportunities for remediation in two of the three information systems we tested.

- Banknote Inventory Tracking System (BITS). BITS tracks various security items related to currency development, performance, and production. The system lacks formal documentation of its configuration and security settings.
- Research and Statistics (R&S) Recruiting. R&S Recruiting processes personally identifiable information of job candidates for research positions across the Board. The system stores configuration information across multiple files but lacks an authoritative baseline as well as formal documentation for configuration management.

These control weaknesses may affect the Board's ability to effectively identify and respond to unauthorized system changes. For example, without documented baselines, the Board may not be able to identify when system configurations deviate from approved secure states, and configuration drift might go undetected.

We also have additional concerns involving all three systems we tested—BITS, R&S Recruiting, and One Agile Supervision Solution, a repository of confidential information related to the supervision of financial institutions. We shared our recommendations to address these concerns as part of recently issued audit reports.

Action Needed

We have two recommendations for the Board to strengthen configuration management practices by establishing and maintaining approved system baseline configurations and improving related configuration management processes. The Board agreed with our recommendations and outlined its planned actions to address them. We will follow up to ensure that the recommendations are fully addressed.

November 10, 2026
Audit Report
2026-IT-B-019