

Federal Reserve: Security Control Review of Select Information Systems

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

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.

Contents

Introduction 4

Objective, Scope, and Methodology 4

Background 5

Finding: Lack of Formal Configuration Documentation Increases the Risk of Undetected Configuration Changes 7

Additional Concerns 9

Weaknesses in Vulnerability Management Oversight Increase Risk of System Exploitation 9

Manual OASIS Access Recertification Process Increases Risk of Unauthorized Access 10

Conclusion and Recommendations 11

Agency Response and Our Evaluation 12

Appendix A: Scope and Methodology 13

Appendix B: Agency Response 15

Abbreviations 18

Introduction

The Federal Reserve System fulfills five general functions essential to promote the effective operation of the U.S. economy and the public interest, including conducting monetary policy, promoting financial system stability, ensuring the safety and soundness of financial institutions, fostering payment system efficiency, and promoting consumer protection and community development. In support of these critical functions, several divisions of the Board of Governors of the Federal Reserve System maintain specialized systems and capabilities that enable the institution to carry out its diverse responsibilities.

This report examines three such Board systems:

- The Banknote Inventory Tracking System (BITS), managed by the Division of Reserve Bank Operations and Payment Systems, tracks various security items related to currency development, performance, and production.
- Research and Statistics (R&S) Recruiting processes applications containing personally identifiable information from candidates for research positions across Board divisions.
- The One Agile Supervision Solution (OASIS) system, operated by the Division of Supervision and Regulation, contains confidential information related to the Board's and Federal Reserve Banks' supervision of financial institutions.

A cybersecurity breach or compromise of these systems could expose confidential supervisory information or personal information, impair banking oversight, or disrupt technical work related to currency.

Objective, Scope, and Methodology

Our objectives were to evaluate the effectiveness of the Board's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

We used a judgmental, nonstatistical sampling approach to select three systems for detailed review: BITS, R&S Recruiting, and OASIS. We selected BITS to represent systems supporting core mission or business functions in the Federal Information Security Modernization Act of 2014 (FISMA) inventory. We selected R&S Recruiting to assess controls in a cloud environment, including considerations related to shared responsibility, third-party service, and cloud-specific risks. We selected OASIS to represent systems in the separately maintained Board Trust Model

(BTM) inventory and to evaluate controls over a system that is maintained on the Board's behalf by a Reserve Bank.[1]

To evaluate security controls for these systems, we

- analyzed security policies, procedures, and documentation
- interviewed relevant Board and System management and staff
- observed and tested specific security processes and controls
- conducted operating system, database, and web application scans[2]

Our review focused on key controls for audit and accountability, access control, and configuration management. For more details on our scope and methodology, see appendix A.

Background

FISMA requires the Board to develop, document, and implement an information security program. FISMA also requires that we conduct an annual, independent evaluation to determine the effectiveness of the Board's information security program, including testing controls for selected systems.

Our review focused on three information systems, BITS, R&S Recruiting, and OASIS, which support different aspects of the Board's mission. Table 1 summarizes the differing system type, ownership, and purpose of the systems we reviewed.

[1] The BTM documents the alignment of the Board's and the Reserve Bank's information security policies, standards, and supporting processes and serves as a formal agreement between the two organizations based on an understanding of differences and similarities between their information security programs. The BTM is intended to support routine exchange of data and information across organizational boundaries and to permit reliance on the information security program of the partner organization.

[2] Due to the sensitivity of vulnerability scan results, we provided these results directly to system stakeholders in a separate, restricted document.

Table 1. Summary of Systems Assessed

System	Type	Division	System description
BITS	Commercial off-the-shelf business application	Division of Reserve Bank Operations and Payment Systems	Tracks security items (for example, banknote, ink, paper, polymer, and plates) according to its project agency and physical locations to support banknote development, performance, and production.
R&S Recruiting	Internally developed	Division of Research & Statistics on behalf of Board research divisions	Processes candidate information for research positions.
OASIS	Cloud and BTM	Federal Reserve Bank of Dallas on behalf of the Division of Supervision & Regulation	Facilitates the end-to-end processes for assessing, monitoring, and rating firms as part of supervision.

Source: OIG analysis.

Finding: Lack of Formal Configuration Documentation Increases the Risk of Undetected Configuration Changes

We identified configuration management documentation weaknesses in BITS and R&S Recruiting, two of the three systems we reviewed. Both systems lack adequate baseline configuration documentation that establishes and defines their approved system configurations. Federal information security standards and configuration management best practices emphasize the importance of establishing, documenting, and maintaining baseline configurations that reflect the current approved state of information systems. Under FISMA, federal agencies are required to comply with National Institute of Standards and Technology standards, which establish that organizations should develop, document, and maintain current baseline configurations with periodic reviews and updates, and document configuration settings.[3]

For BITS, the baseline configuration document primarily describes step-by-step procedures for upgrading to newer software versions, as per the document's stated purpose, rather than establishing a formally reviewed configuration baseline. A system representative informed us that BITS administrators largely rely on vendor default configurations. However, this reliance is not formally documented, including which vendor defaults are accepted or which software version is approved. Additional documentation describing configuration elements is outdated, and we found no evidence of baseline document review since 2023 despite multiple system upgrades.

Configuration Documentation: A Governmentwide Challenge

According to the U.S. Government Accountability Office's 2019 review of federal information security, 14 of 16 agencies reviewed had weaknesses in configuration management activities:

- Nine agencies had gaps in developing, maintaining, or implementing baseline configurations for their information systems.
- Four agencies did not develop baseline configurations for all systems or network devices.
- Two agencies did not review or approve their baseline configurations.

Source: U.S. Government Accountability Office, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545, July 26, 2019.

[3] National Institute of Standards and Technology, *Special Publication 800-53, Revision 5,* CM-2 and CM-6.

For R&S Recruiting, the Advanced Research Computing team stores code and configuration items in its source code repository tool. While the repository contains configuration-related information across multiple files, the system does not designate an authoritative configuration baseline documenting approved security settings, system dependencies, or deployment parameters. These files lack version identifiers, approval records, or named responsible officials. In addition, another system representative confirmed that the Advanced Research Computing team has not developed a configuration management plan.

The Board has established configuration baseline requirements in its *Secure Configuration Baseline Standard*, which requires system owners to develop and document information security configuration settings in a configuration baseline for infrastructure devices, middleware, commercial off-the-shelf business applications, and development platforms. The standard further requires, along with the Board's *Application Development Security Standard*, that internally developed business applications be managed using a documented system development life cycle.

Configuration baseline documentation weaknesses occurred because the Board's standards do not provide system owners with sufficient direction for establishing and documenting authoritative baseline configurations that consistently identify the approved configuration of their system. For example, the Board's *Secure Configuration Baseline Standard* explicitly excludes internally developed applications and, in general, lacks specific content requirements for baseline documentation, such as current software versions or periodic review. For internally developed applications, the *Application Development Security Standard* requires system development life cycle processes but does not mandate baseline documentation. Further, while the *Secure Configuration Baseline Standard* requires automated monitoring or biannual manual review of baselines, it does not require that the baseline documentation be updated when system changes occur.

Without adequate baseline configuration documentation, the Board faces operational security risks. First, when there is staff turnover, version-controlled repositories track configuration changes but new personnel lack authoritative baseline documentation that identifies which configurations represent approved security postures. Second, without documented baselines, the Board cannot identify when system configurations deviate from approved secure states. Configuration drift might go undetected because there is no documented standard against which to compare actual system states, and change management becomes inconsistent without a single baseline to assess the security risk of proposed changes.

Additional Concerns

Two additional concerns warrant the Board's attention. First, we identified vulnerabilities in the systems and infrastructure we tested, including unpatched software flaws, insecure configurations, and end-of-life software, that stem from program-level deficiencies in the Board's vulnerability management governance and oversight. Second, we noted that the OASIS access recertification process relies primarily on manual user and administrator validation. While these conditions present security risks, we are not issuing formal recommendations in this report because our 2026 FISMA report addressed program-level vulnerability management improvements,[4] and OASIS management is already undertaking corrective actions in response to our recommendations from a prior review of OASIS.[5]

Weaknesses in Vulnerability Management Oversight Increase Risk of System Exploitation

We identified vulnerabilities in the web applications, databases, and operating systems for two of the three systems we reviewed. We also identified vulnerabilities on Board-managed infrastructure servers that exchange data with the third system. These vulnerabilities include unpatched software flaws, insecure configurations, and end-of-life software. In addition, we identified vulnerabilities with a known exploit that persisted for months despite being identified in the Board's own scanning reports, and systems operating with overdue vulnerabilities without formal risk acceptance or a plan of action and milestones. We also identified insecure configurations, including outdated encryption protocols, and weak cryptographic ciphers. The Board addressed some of these vulnerabilities after our inquiries rather than through its routine monitoring and escalation processes.

The security weaknesses identified reflect program-level deficiencies in the Board's vulnerability management governance and oversight that extend beyond individual system issues. We found similar weaknesses in our 2026 audit of the Board's information security program, which included recommendations to address those issues.[6] The specific vulnerability scan results for each system have been separately communicated to system officials and management for remediation. In response to our inquiry, system owners took corrective actions, including remediating identified vulnerabilities or providing documentation for vulnerabilities where

[4] Office of Inspector General, *Federal Reserve: 2026 Information Security Program Audit*, OIG Report 2026-IT-B-018, October 28, 2026.

[5] Office of Inspector General, *Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS*, OIG Report 2026-SR-B-001, February 3, 2026.

[6] Office of Inspector General, *Federal Reserve: 2026 Information Security Program Audit*.

immediate remediation was not feasible. As such, we are not issuing any system-specific recommendations.

Manual OASIS Access Recertification Process Increases Risk of Unauthorized Access

During our review of the OASIS annual recertification process, we noted that, although user access to OASIS is automatically revoked upon an employee's termination, users and local administrators manually validate continued need for system access. OASIS management is already undertaking corrective actions in response to our recommendations to strengthen the access recertification process from a prior review of OASIS. As part of the February 2025 annual access recertification, the Board validated 410 OASIS accounts and identified 159 of those accounts (39 percent) as inactive. Reviewers also identified access exceptions and users with outdated or unnecessary permissions.

In our February 2026 report, we made several recommendations to OASIS management to improve access controls.[7] Among them, we recommended the Board develop guidance that describes the expectations for performing the agency's annual access review process, including designating responsibility for performing the attestation to individuals with knowledge of the user's roles and responsibilities, such as the user's supervisor or other possible alternatives. OASIS management informed us that they were undertaking corrective actions to address this recommendation. As such, we are not issuing additional recommendations but will continue to monitor OASIS access controls for safeguarding confidential supervisory information as part of future recommendation follow-up efforts.

[7] Office of Inspector General, *Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS*, OIG Report 2026-SR-B-001, February 3, 2026.

Conclusion and Recommendations

Based on our review of selected security controls from the access control, audit and accountability, and configuration management control families for BITS, R&S Recruiting, and OASIS, as well as a system authorization control for the R&S Recruiting system, we identified areas where control practices aligned with established requirements and areas where improvements are needed. The results and any associated recommendations are limited to the specific controls, systems, and evidence examined during the review. Accordingly, the review was not designed to, and does not provide, an assessment of the overall effectiveness of the security control environment for BITS, R&S Recruiting, and OASIS, nor should the results be interpreted as assurance regarding controls outside the scope of the review.

We recommend that the BITS and R&S Recruiting system managers, at the direction of the system owners

1. Establish and maintain a documented and approved baseline configuration that reflects the approved system configurations for all system components.

We recommend that the R&S Recruiting system owner

2. Develop and implement a configuration management plan that includes
    a. secure configuration settings.
    b. roles and responsibilities for configuration management.
    c. change control and configuration management processes.

Agency Response and Our Evaluation

In response to our official draft report, the director of the Division of Research and Statistics, the acting director of the Division of Reserve Bank Operations and Payment Systems, and the director of the Division of Supervision and Regulation agreed with our finding and recommendations and conveyed the Board's commitment to addressing our recommendations. The Board's formal response to the report is included in its entirety in appendix B.

The actions described by the division directors appear to be responsive to our recommendations. We will follow up with the Board quarterly to ensure that the recommendations are fully addressed.

Appendix A: Scope and Methodology

Our objectives were to evaluate the effectiveness of the Board's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

To accomplish these objectives, we used a judgmental nonstatistical sampling approach to select 3 systems from a population of 342 systems. The systems we selected were OASIS, a BTM cloud system; BITS, a business application; and R&S Recruiting, an internally developed application for recruiting for research positions across the Board. The selection was designed to ensure representation across key system types and operational environments rather than to achieve statistical representativeness.

We selected the systems judgmentally because the objective of our review was to assess the design and implementation of controls across diverse system categories, not to project results across the entire population. In making the selections, we considered factors like system classification (FISMA versus BTM managed by the Federal Reserve Bank of Dallas), hosting model (on premises versus cloud), functional role (business applications versus infrastructure/technical system), risk profile, and operational significance. This judgmental selection approach was intended to provide a cross-sectional assessment of controls across materially different system types and environments. As such, the results of our sample cannot be projected to the full population of systems.

In addition, we reviewed the effectiveness of selected information security controls (table A-1). Our review primarily focused on selected security controls from three control families: access control (AC), audit and accountability (AU), and configuration management (CM). These security control families were selected using a risk-based methodology that prioritized FISMA-related controls from the identity and access management and the CM domains as well as related control enhancements to support our 2025 FISMA audit. Additionally, the CA-6 (authorization process) control was added to our R&S Recruiting review based on risk after we determined during initial testing that further assessment of the system authorization process was necessary.

Table A-1. Security Controls Assessed by System

Control		System		
Number	Name	OASIS	BITS	R&S Recruiting
AC-2	Account Management	In scope	In scope	In scope
AC-5	Separation of Duties	In scope	Out of scope	In scope
AC-6	Least Privilege	In scope	Out of scope	In scope
AC-6(2)	Least Privilege—Nonprivileged Access for Nonsecurity Functions	In scope	Out of scope	In scope
AC-6(9)	Least Privilege—Log Use of Privilege Functions	In scope	Out of scope	In scope
AC-8	System Use Notification	In scope	In scope	In scope
AU-2	Event Logging	In scope	In scope	In scope
AU-3	Content of Audit Records	In scope	In scope	In scope
AU-6	Audit Record Review, Analysis, and Reporting	In scope	In scope	In scope
AU-6(1)	Audit Record Review, Analysis, and Reporting—Automated Process Integration	In scope	Out of scope	In scope
AU-11	Audit Record Retention	In scope	In scope	In scope
CA-6	Authorization	Out of scope	Out of scope	In scope
CM-2	Baseline Configuration	In scope	In scope	In scope
CM-6	Configuration Settings	In scope	In scope	In scope
CM-8	System Component Inventory	In scope	In scope	In scope
CM-9	Configuration Management Plan	In scope	Out of scope	In scope

Source: OIG analysis.

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted this work from March 2025 to October 2026.

Appendix B: Agency Response



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

October 23, 2026

Michael VanHuysen
Associate Inspector General for Audits and Evaluation
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Mr. VanHuysen:

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG) draft report titled *Federal Reserve: Security Control Review of Select Information Systems*. We appreciate the OIG's work to develop the report and the recommendations.

We concur with the OIG's recommendations to strengthen system management by ensuring approved configuration baselines are documented for all system components and that configuration plans include secure configuration settings; roles and responsibilities; and change control processes. In support of these actions, the Division of Information Technology is updating its configuration management and application development policies and standards to ensure configuration baseline and configuration management plan requirements are clearly communicated to system owners. In addition, as noted under *Additional Concerns*, the Board is strengthening its vulnerability management program through the implementation of Binding Operational Directive (BOD) 26-04.

Supervision and Regulation concurs with the observation that the manual access certification process within OASIS requires continued improvement and appreciate OIG's acknowledgment of corrective actions already underway. Consistent with the guidance provided during the OIG's prior engagement[1], the OASIS Program has been actively working to strengthen both internal and external access review processes. While these reviews remain manual in nature at this stage, the new process aligns with the Federal Reserve's access review requirements and clearly defines access review and approval roles and responsibilities.

With respect to the 159 inactive accounts:

[1] OIG Memorandum Report 2026-SR-B-001: *Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS.*

www.federalreserve.gov

1. Inactive Account Status: Accounts identified as "inactive" are disabled and cannot access the OASIS portal. These accounts remain subject to ongoing monitoring even while disabled.
2. Reactivation Controls: A defined process with required approvals governs the reactivation of any inactive account, ensuring that access is not restored without appropriate authorization and oversight.

Consistent with the management response noted in the February 3, 2026 report, the OASIS Program expects to complete execution of the enhanced access review process by year-end 2026.

We appreciate your professionalism and diligence during the audit. We look forward to continuing to work with your office in the future.

Regards,

STACEY TEVLIN
Digitally signed by STACEY TEVLIN
Date: 2026.10.23 10:34:57 -04'00'

Stacey Tevlin
Director of the Division of Research and Statistics

SUSAN FOLEY
Digitally signed by SUSAN FOLEY
Date: 2026.10.22 21:18:50 -04'00'

Susan Foley
Acting Director of the Division of Reserve Bank Operations and Payment Systems

RANDALL GUYNN
Digitally signed by RANDALL GUYNN
Date: 2026.10.27 17:31:48 -04'00'

Randall Guynn
Director of the Division of Supervision and Regulation

cc: Jeff Riedel
Charles Young
John Stevens
Caio Peixoto
Susmit Patel

Response to recommendations presented in the Draft OIG Audit Report, *"Federal Reserve: Security Control Review of Select Information Systems"*

Finding 1:

Recommendation 1:
We recommend that the BITS and R&S Recruiting system owners establish and maintain a documented and approved baseline configuration that reflects the approved system configurations for all system components.

Management Response:
We concur with the finding and recommendation. The BITS and R&S Recruiting system owners through their system managers will update system documentation to include approved baseline configurations that reflect the approved system configuration for all system components. Target date: Q1 2027.

Recommendation 2:

We recommend that the R&S Recruiting system owner develop and implement a configuration management plan that includes

a. secure configuration settings.

b. roles and responsibilities for configuration management.

c. change control and configuration management processes.

Management Response:
We concur with the finding and recommendation. The R&S Recruiting system owner through their system manager will update system documentation to include a configuration management plan that includes secure configuration settings; roles and responsibilities; and change control and configuration management processes. Target Date: Q1 2027.

Abbreviations

AC	access control
AU	audit and accountability
BITS	Banknote Inventory Tracking System
BTM	Board Trust Model
CM	configuration management
FISMA	Federal Information Security Modernization Act of 2014
OASIS	One Agile Supervision Solution
R&S	Research and Statistics



Hotline

Report fraud, waste, abuse, and mismanagement involving the programs and operations of the Board or the CFPB.

oig.federalreserve.gov/hotline

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

1-800-827-3340

General Contact

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov