Evaluation Report
2026-MO-B-010R
July 15, 2026

Board of Governors of the Federal Reserve System

The Board Needs a More Robust Insider Risk Management Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2026-MO-B-010R, July 15, 2026

The Board Needs a More Robust Insider Risk Management Program

Findings

The Board of Governors of the Federal Reserve System's insider risk management (IRM) activities do not proactively or effectively identify and manage risks to the agency's information and assets. The Board's IRM activities are not consistent with leading practices for designing and operating IRM programs. We also identified a maturity gap between the Board's IRM activities and a peer federal financial regulatory agency's IRM program. These weaknesses are further demonstrated by the Board's handling of recent potential insider risk incidents.

In addition, the Board lacks (1) a process to identify its critical assets, (2) a centralized IRM program to proactively identify and manage insider risks at an enterprise level, (3) procedures for the timely sharing of pertinent information internally and with the Federal Reserve System, (4) enterprise-level policies and procedures establishing consistent incident response and reporting practices, and (5) insider risk training requirements for all Board staff.

Recommendations

We have nine recommendations that will contribute to developing a more robust IRM program commensurate with the risks presented by the scope and breadth of the Board's activities as the nation's central bank. In its response to our draft report, the Board concurred with our recommendations and outlined actions to address each recommendation. We will follow up to ensure that the recommendations are fully addressed. Given the sensitivity of the information in our review, portions of the public version of this report have been redacted.

Purpose

We conducted this evaluation to assess the design and effectiveness of the Board's IRM activities. We evaluated the Board's governance and management of its activities to detect, deter, and mitigate insider risks, and assessed whether the Board's IRM activities align with leading practices. We also assessed the Board's and the System's information sharing and coordination on insider risk topics and incidents. We did not assess System IRM activities conducted by the Federal Reserve Banks.

Background

Given the Board's role as the nation's central bank and the Federal Open Market Committee's monetary policy activities, the Board must manage an evolving and dynamic set of internal and external risks to the System's operations. These risks include those presented by insiders and foreign adversaries that could degrade the effectiveness of the Board's operational activities and potentially harm the U.S. economy. To address the threat posed by insiders, entities in the U.S. government, academia, and the private sector have identified leading IRM practices that help to mitigate these risks.

Recommendations, 2026-MO-B-010R, July 15, 2026

The Board Needs a More Robust Insider Risk Management Program

Finding 1: The Board Should Identify and Assess Its Critical Assets

Number	Recommendation	Responsible office
1	Define the Board's critical and unique assets and assess the risks to those assets.	Office of the Chief Operating Officer

Finding 2: The Board Should Centralize Its Enterprise IRM Activities

Number	Recommendation	Responsible office
2	Establish a centralized IRM program, or hub, to collect and analyze information from all agency sources to identify insider risks related to the Board's critical assets. The IRM program should initiate appropriate responses to resolve identified concerns including a. a senior official or oversight group accountable for overseeing the agency's IRM program. b. documented governance processes and structures in bylaws and committee charters. c. clear escalation expectations for communicating with the Board of Governors and appropriate committees. d. members consisting of program stakeholders from a broad range of functional areas, including stakeholders with specialized disciplinary expertise, to strengthen insider risk processes. e. a dedicated insider risk budget that provides for staffing, analytic, and technology assets necessary to maintain and improve effectiveness in fulfilling its objectives.	Office of the Chief Operating Officer

Finding 3: The Board Should Establish Procedures to Timely Share Relevant Insider Risk Information Internally and with the System

Number	Recommendation	Responsible office
3	Establish information sharing procedures between Board divisions and the centralized hub that a. direct components responsible for intelligence, security, human resources, and other relevant areas to establish reporting guidelines to provide IRM personnel regular and timely access to necessary information. b. direct relevant Board components to establish automatic sharing of information, or repeatable and sustainable processes for sharing necessary information to identify, analyze, and resolve insider risks. c. require a periodic review of IRM program information sources and past insider risk inquiries to assess the relevance and utility of the sources of information and indicators. d. establish clear lines of reporting and collaboration with System stakeholders, including RBOPS, National IT, and Reserve Bank IRM programs.	Office of the Chief Operating Officer

4	Ensure the centralized hub has timely access, as permitted, to available federal intelligence and counterintelligence reporting information, such as analytic products pertaining to adversarial threats.	Office of the Chief Operating Officer

Finding 4: The Board Should Establish Enterprisewide Insider Risk Policies and Procedures

Number	Recommendation	Responsible office
5	Establish policies and procedures for assessing and responding to insider risks involving both classified and unclassified information that a. centralize IRM program responses. b. balance the need for oversight reviews from legal and civil liberties and privacy officials. c. provide appropriate and consistent due process and fairness procedures for disciplinary actions. d. establish guidelines and procedures for records retention. e. establish clear thresholds for referrals to the OIG and external law enforcement officials.	Office of the Chief Operating Officer
6	Establish internal reporting sites for cleared and uncleared employees to refer potential concerns or incidents to the IRM program.	Office of the Chief Operating Officer
7	Define program objectives, including a strategic vision, and establish metrics to measure progress toward achieving them. When identifying areas requiring improvement for senior leadership, the program should a. use trends and baselines to establish criteria for anomalous behavior. b. create formal feedback loops from responders to the IRM program to keep it informed of matter resolution, request clarifying information, and aid deconfliction among internal and external stakeholders. c. develop guidelines and procedures for documenting each insider risk matter and response action taken, including an incident repository to capture lessons learned. d. establish oversight mechanisms or procedures to ensure proper handling and use of records and data and to ensure that access to such records and data is restricted to program personnel.	Office of the Chief Operating Officer

Finding 5: The Board Should Require IRM Training for All Board and IRM Personnel

Number	Recommendation	Responsible office
8	Designate staff to serve as insider risk analysts and provide them with relevant training to develop IRM skills and competencies, including a. requiring all IRM program personnel to have some level of formal training in counterintelligence and security principles, techniques, and tools, including behavioral science perspectives and expertise. b. requiring all IRM program personnel to be fully trained in applicable laws and regulations regarding records retention, civil liberties, and privacy laws. c. providing continuing education and training in appropriate fields and disciplines.	Office of the Chief Operating Officer
9	Require that all Board personnel take IRM training annually.	Office of the Chief Operating Officer

Contents

Introduction

Objective

Our objective was to assess the design and effectiveness of the Board of Governors of the Federal Reserve System's insider risk management (IRM) activities. Our evaluation covered the Board's governance and management of activities to detect, deter, and mitigate insider risks, including information sharing and coordination with the Federal Reserve System, and assessed whether the Board's IRM activities align with leading practices. We did not assess IRM activities conducted by the Federal Reserve Banks. Appendix A provides additional details about our scope and methodology.

Background

An *insider threat* is the potential for an individual who has or had authorized access to an organization's critical assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization, including workplace violence. Insiders include employees, contractors, consultants, and trusted external entities.[1] An *insider risk* is the likelihood and effect of an insider threat being realized.

Critical assets include an organization's people, processes, information, technology, and facilities that, if destroyed, altered, or otherwise degraded, would impair the assets' confidentiality, integrity, or availability and have severe negative effects on the organization's support of its essential missions and business functions. Such assets may include key internal business processes, negotiation strategies, and proprietary research and formulas.

An *IRM program* is a designated set of capabilities and resources allocated to mitigate insider threats and manage insider risks. These programs provide a central hub to analyze enterprise insider risks, detect and respond to incidents, and leverage pattern detection and information to proactively prevent incidents.

Insider Risks Across the Federal Government

There have been several well documented and public instances of individuals with authorized access to sensitive information at federal agencies—including the Board—jeopardizing national security and U.S. citizens' safety by sharing that information with outsiders.

To address insider risks, a 2011 executive order directed structural reforms to ensure responsible sharing and safeguarding of classified information.[2] It established the National Insider Threat Task Force (NITTF)

[1] The definitions for *insider threat*, *insider risk*, *critical assets*, and *IRM program* are from Software Engineering Institute (SEI), *Common Sense Guide to Mitigating Insider Threats*, Carnegie Mellon University, September 15, 2022. According to its website, the Software Engineering Institute at Carnegie Mellon University is a federally funded research and development center—a nonprofit, public–private partnership that conducts research for the U.S. government.

[2] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011.

to develop policies and standards for agencies to create insider threat programs.[3] Because many agencies handle unclassified information that those organizations consider extremely sensitive and critical, NITTF's most recent best practices guidance states that agencies should consider expanding the scope of insider threat program activities to include unclassified information consistent with mission needs.[4]

Threats to the Board's Information and Infrastructure

Given the Board's role as the nation's central bank and the Federal Open Market Committee's (FOMC) monetary policy activities, the Board's proprietary economic analysis and data are of great interest to foreign adversaries. The Board must manage an evolving and dynamic set of internal and external risks to the System's operations, including risks from insiders and foreign adversaries that could have detrimental effects to its operations and the economy.[5] Further, foreign intelligence entities increasingly focus their activities on intellectual property, research, and economic strategies to undermine U.S. competitiveness and weaken national security.[6]

- **(U//FOUO//TLP AMBER + STRICT)** [redacted]
- **(TLP GREEN)** [redacted]
- **(U//FOUO//TLP GREEN)** [redacted]

[3] Presidential Memorandum, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, November 21, 2012.

[4] National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*, 2024.

[5] U.S. Department of the Treasury, *Financial Services Sector Risk Management Plan*, January 2025.

[6] Sentinel Research, *Perceptions of Counterintelligence in Corporate and Academic Sectors*, November 2025.

EXFILTRATION OF SENSITIVE BOARD AND FOMC INFORMATION

A then-Board employee, now retired, shared sensitive Board and FOMC information and other documents with Chinese security and intelligence operatives beginning in 2017.

There have been instances in which insiders at the Board have compromised information about the Board's mission-related responsibilities and processes, including highly sensitive and potentially market-moving information like nonpublic FOMC interest rate setting information and deliberations, bank supervision stress test information, and other proprietary economic analysis (see sidebars throughout this report).

Despite these incidents, a senior Board official told us that the Board has been resistant to adopting a comprehensive insider risk program because the current ad hoc approach allows each division to respond to incidents based on its own security needs and the particular information or asset that the division is responsible for protecting.

In response to a recommendation we made in 2016 that remains open, the Board's Division of Information Technology enlisted a third-party vendor in November 2024 to develop a strategy for creating an unclassified IRM program.[7] A study by the third-party vendor found that the academic, traditional nature of the Board's work, combined with the benefits of engaging with foreign nationals, has deepened a cultural environment in which adoption of insider risk indicators and warnings is viewed as punitive or unnecessary. Separately, the Division of Reserve Bank Operations and Payment Systems (RBOPS) reviewed IRM practices for Reserve Banks and System entities, including the nationwide Federal Reserve National Information Technology (National IT)[8] and Federal Reserve Financial Services. Its report had similar conclusions to our report and found that the System needs to identify its critical assets, standardize separate IRM programs, establish a governance structure, and create a framework to share employee termination information across the System.

Leading IRM Practices

To assess the Board's incident response and IRM activities, we developed a list of leading practices for IRM programs derived from the intelligence community, academia, private sector, and our prior work.[9]

[7] We recommended in 2016 that the Division of IT work with the Board's chief operating officer to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agencywide insider threat strategy for sensitive but unclassified Board information, as appropriate. Because our recommendations in this report include each of the Board's various IRM efforts and reflect the latest leading practices in the evolving IRM landscape, these recommendations will supersede our 2016 recommendation. See Office of Inspector General, *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016.

[8] National IT is a nationwide team that delivers technology solutions and support across the System.

[9] Given the Board's broad responsibilities and unique governance structure, the leading practices we reviewed consist of National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*; National Insider Threat Task Force, *Protect Your Organization from the Inside Out: Government Best Practices*, 2016; National Insider Threat Task Force, *Insider Threat Program Maturity Framework*, November 1, 2018; Office of Inspector General, *Strengthening Organizational Governance*, OIG Insights, February 14, 2019; Securities Industry and Financial Markets Association, *Insider Threat Best Practices Guide*, 3rd Edition, July 2024; and Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*.

These leading practices include centralizing management of enterprise and insider risks to a single hub that gathers, integrates, analyzes, and responds to potential insider risk information and incidents. Mature IRM programs have

- clear governance, organizational design, and dedicated budget
- established policies and procedures
- information access and sharing procedures
- training for IRM staff and agency personnel
- records retention procedures
- information processing and analysis procedures

Other leading practices for these programs include developing policies and procedures that ensure civil liberty protections and provide enterprise program metrics for evaluation, establishing reporting guidelines for other parts of the organization to timely share valuable information across the agency, and creating formal feedback loops and referral processes. For a full list, see the summary of our testing results against leading practices below.

Peer Federal Financial Regulatory Agency

We benchmarked with a peer federal financial regulatory agency's IRM program to understand its practices for managing relevant risks. The peer agency's program incorporates such leading practices as

- establishing a centralized hub with a dedicated program manager and policies and procedures, including reporting metrics, training, and records retention requirements
- establishing information access and sharing procedures to facilitate the hub's IRM processing and analysis

The Board Has Four Separate Programs to Respond to Information Security Incidents, But No Centralized Entity with Decisionmaking Authority

Unlike a peer financial regulatory agency, which operates a centralized IRM program, four divisions at the Board have separate programs that focus on information security activities. While the divisions use various terms, each program conducts some level of IRM activities. For the purposes of this report, we generally refer to the efforts of these four programs as *IRM activities*. These programs include the Office of the Chief Operating Officer's Insider Threat Program within its Intelligence, Insider Risk, and National Security Programs (IINS) group; the Division of IT's Incident Response Program; and the FOMC's Program for Security of FOMC Information, which is facilitated by the FOMC Secretariat in the Division of Monetary

Affairs. In addition, the Division of Supervision and Regulation's (S&R) Security Incident Management Program conducts IRM-related activities to support the Division of IT's Incident Response Program.[10]

IINS operates a fully accredited insider threat program for classified information, while the other three programs protect different types of unclassified information, such as FOMC, confidential supervisory information (CSI), personally identifiable information, and other sensitive Board and System information. A senior Board official stated that these silos stem from each program being developed independently as a result of the specific responsibilities of those divisions.

The Board's governance structures and responsibilities for these four programs are not well developed in agency policies and governance documents.[11] The administrative governor, who chairs the Committee on Board Affairs, delegated to the chief operating officer (COO) the authority to formulate, approve, and implement policies pertaining to administrative oversight of the Board's operations and resources, including information technology and security, and handling of classified information. However, this delegation does not include the S&R and FOMC programs. Our analysis of Board policies and governance documentation found that no individual or Board committee is specifically accountable for leading and overseeing the collective insider risk activities for the Board.

In addition, each of the four separate programs has different resources, staff, leadership, and response processes, and there is no centralized coordination, oversight, or decisionmaking body related to these activities (table 1). For example, the Division of IT, FOMC Secretariat, and IINS programs each have a separate group of senior leaders who convene to assess the severity of an identified incident and to determine next steps, while the S&R program forwards confirmed or suspected incidents involving confidential information to the Division of IT program. The Division of IT, under Board policy, will promptly inform the Core Response Group of (a) security incidents that involve an information system that stores or maintains Board data; (b) known or suspected security incidents involving information rated Restricted FR or Restricted-Controlled FR; (c) known or suspected privacy breaches involving sensitive personally identifiable information; (d) any incident that it believes may constitute a major incident; and (e) any other incident that it, in consultation with the COO and appropriate staff of the Legal Division, believes merits Core Response Group review.[12] The Core Response Group, which consists of the COO, the chief information officer, the senior agency official for privacy, the information security officer,

[10] Senior Board officials explained that the additional IRM activities conducted by the S&R program developed as the result of a need to ensure Reserve Bank compliance and reporting for information security incidents related to Board-delegated activities under the Division of IT's Incident Response Program. As of March 22, 2026, all employees and contractors from S&R's Operations IT function and Program Management Office, which includes the Security Incident Management Program, moved to the Division of IT.

[11] Strengthening organizational governance, including establishing an enterprisewide approach for managing risks and administering certain business functions, continues to be a major management challenge for the Board. See Office of Inspector General, *2025–2026 Major Management Challenges for the Board*, OIG Report, April 30, 2025.

[12] The Board's information security officer or, for privacy breaches, the Board's senior agency official for privacy, may, at their discretion, notify the Core Response Group of a security incident that involves a loss of a Board or Reserve Bank device that meets the Board's encryption requirements; involves a loss within the System only; or involves a loss where an email is misdirected to a federal, state, or foreign regulatory agency or a financial institution regulated by the Board.

the general counsel, the inspector general, a congressional liaison officer, and a public affairs officer, advises the administrative governor on responding to referred security incidents.[13]

[13] The COO chairs the Core Response Group and the senior agency official for privacy chairs the Core Response Group for all privacy breaches.

Table 1. Board IRM Activities

Scope of responsibility	Responsible official	Dedicated staff	Program budget	[redacted]	Incident procedures
IINS					
Protect classified information	COO	3 part-time staff	No	[redacted]	Conducts inquiries into classified incidents and may work with other Board divisions on unclassified incidents when authorized by the Executive Intelligence Oversight Group. [redacted]
Division of IT					
Identify and respond to information security incidents involving Board information, including personally identifiable information	Chief information officer	5 full-time staff	No	[redacted]	Reviews alerts and other information about potential cybersecurity incidents. [redacted]
FOMC Secretariat					
Protect FOMC information at the Board and across the System	FOMC Secretary	0.35 full-time equivalents	No	[redacted]	Reviews potential incidents involving FOMC information, coordinates with the responsible division or Reserve Bank, and convenes the FOMC Incident Response Group or National IT when an escalation is required.
S&R					
Protect CSI at the Board and Reserve Banks and notify the Division of IT	S&R chief information officer	1 full-time staff	No	[redacted]	Reviews, through an incident response group, potential incidents; coordinates with the responsible Reserve Bank; and escalates confirmed or suspected incidents related to CSI to the Division of IT.

Source: OIG analysis.

Operationally, the S&R and FOMC Secretariat programs rely primarily on the Division of IT's tools and capabilities to detect insider incidents, such as data loss prevention, user activity monitoring, and suspicious email alerts, among others. Given these monitoring capabilities, the Division of IT's tools typically serve as the initial detection point for potential unclassified incidents. However, coordination between these programs after an incident is detected is narrow and limited to specific circumstances, such as when an incident involves multiple divisions or programs.

The Board conducts limited activities to proactively identify and prevent insider risks. [redacted] Finally, while these programs' overall goals overlap, coordination among the programs is limited and individual program efforts often proceed in a siloed manner.

Summary of Testing Results Against Leading Practices

We evaluated the Board's IRM activities in comparison to leading practices derived from the intelligence community, academia, private sector, and our prior work in the six areas listed below. We also reviewed recent incidents and benchmarked with a peer federal financial regulatory agency to further compare the maturity of the Board's IRM activities.

Governance and Organizational Design

Leading practices. Establish a centralized hub and designate a senior official, among other centralization and formalization actions.

Results. The Board does not have a clearly documented governance structure or a designated senior official who oversees these activities. Further, the Board lacks a centralized hub led by a designated official with dedicated staff and resources responsible for enterprisewide gathering, integrating, analyzing, and responding to potential insider risk information and incidents. In addition, the Board has not identified its most critical assets or assessed the risks to those assets. As such, it cannot tailor its program activities to protect the identified assets.

Policies and Procedures

Leading practices. Develop governance processes, policies, and procedures that identify key roles and responsibilities, budgets, staffing levels, disciplinary actions, key performance metrics, and actions to address insider threats.

Results. All four of the Board's separate programs outline the individual governance processes and program activities in policies and procedures. In addition, the incident response oversight groups for the four programs contain overlapping membership. However, the Board lacks a single IRM policy for both

[redacted]

unclassified and classified information, formalized due process procedures in the event that someone is identified as a potential insider threat, and detailed consequences for information security violations.

Information Access and Sharing

Leading practices. Establish reporting guidelines and repeatable processes for insider risk personnel to share, receive, and review information timely and automatically.

Results. There is no broad information sharing across the four programs. None of the Board's programs have ready access to all types of information relevant to insider risk incidents.

Training

Leading practices. Require all personnel to take insider threat training and provide continuing education and training in various fields and disciplines to insider risk personnel.

Results. Only the IINS program requires its personnel to be trained in specific counterintelligence and security principles. Further, the Board does not require personnel without security clearances to take general insider risk training.

Records Retention

Leading practices. Establish oversight mechanisms and procedures for retaining records and documents.

Results. The Division of IT documents confirmed information security incidents in a System database. [15] The other three programs have established guidelines and procedures for retaining records and documents related to an incident.

Information Processing and Analysis

Leading practices. Develop guidelines to document programmatic actions taken, which include formal feedback loops, thresholds for referrals to internal and external entities, criteria for anomalous behavior, and capturing lessons learned.

Results. The Division of IT's program has the most tools to detect and address incidents,

[15] The Federal Information Security Modernization Act of 2014 defines an *incident* as something that (a) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system or (b) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

[redacted] The FOMC Secretariat, IINS, and S&R programs have guidelines and procedures for documenting incident response actions and resolutions, such as annual reporting or incident databases. The Board's three programs for unclassified information (in the Division of IT, FOMC Secretariat, and S&R) lack a standard approach for referring incidents or potential risks to outside entities, such as the Office of Inspector General or the Federal Bureau of Investigation. Further, only the IINS program clearly outlines when to report employee threats of violence. Although all four programs review and capture lessons learned from previous incidents, [redacted] the Board does not centralize, aggregate, and disseminate these lessons learned across the enterprise.

Finding 1: The Board Should Identify and Assess Its Critical Assets

The Board lacks a process to identify and assess its critical assets. Leading practices state that agencies should identify their critical assets and assess the risks to those assets. However, the siloed nature of the Board's four programs and the lack of a consolidated IRM hub have contributed to the Board not formally identifying its critical assets, which may cause the agency to overlook its most salient risks and vulnerabilities.

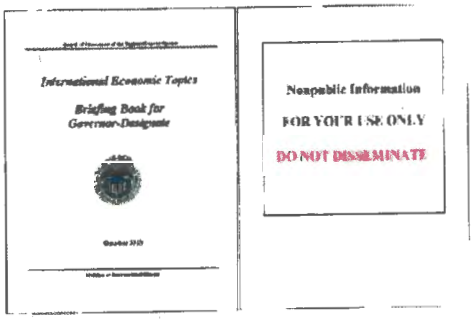
The Board Has Not Identified Its Critical Assets

The Board has no enterprise-level consensus about which of its assets are most critical (see sidebar). The agency also does not have a process to evaluate risks to those assets.[16] Senior Board officials identified differing information types or functions that they informally consider critical assets. Examples include market-moving sensitive economic information (for example, Class I FOMC), the global dollar payment system, Federal Reserve banknotes, and the System's custodial services for foreign central banks—none of which fit neatly into one of the Board's siloed programs.

CRITICAL ASSETS ARE VALUABLE INTELLIGENCE

A recent potential insider risk incident involved the exfiltration of information relating to Federal Reserve forecasts and economic analysis, including confidential briefing books for recently nominated Board governors (figure 1).

Figure 1. Example of Confidential Briefing Book



Source: Board of Governors of the Federal Reserve System, *Briefing Book for Governor-Designate*, October 2018, and OIG analysis.

In addition, the RBOPS report of System IRM found a lack of uniformly identified critical assets. An RBOPS official opined that the System would benefit from the Board assessing critical assets Systemwide, since the System handles critical functions like the payment systems.

[16] The third-party vendor's analysis of the Division of IT's unclassified information protection systems also found that the Board has not identified its critical assets.

Leading Practices Call for Identifying Critical Assets and Assessing Risk

According to leading practices, agencies should establish a process to identify critical and unique assets and assess the risk to those assets. An organization's critical assets are more than sensitive information and may include people, facilities, or other elements that contribute to the Board's essential systems or processes. Further, the NITTF recognizes that many government agencies possess extremely sensitive and critical information even though the information may not be classified. For example, a peer federal financial regulatory agency created a list of its critical information used to assess the severity of potential information security incidents.

The Board's Siloed Approach May Overlook Risks and Vulnerabilities

Although the Board has policies that identify critical mission functions, operations, or information in need of protection, the siloed nature of the Board's four programs and the lack of a consolidated IRM hub has contributed to the Board not identifying its critical assets at an enterprise level. Board officials agreed with our assessment that there is no enterprise list of critical assets. Further, they agreed that various Board and System documentation identify many assets and mission-essential functions, which could serve as a foundation to aggregate and assess critical assets.

(TLP: AMBER + STRICT) [redacted] When identifying its most critical assets, the Board should consider which information and data may be of interest to foreign adversaries and how they may be combined to increase the potential consequences.

Because the Board has not engaged in a formal process to identify its most critical assets, the Board's current ad hoc approach may inadvertently overlook some of the most salient risks and vulnerabilities agencywide. The Board must first define its critical assets and the associated risks to those assets before it can design an enterprisewide IRM program, establish Boardwide policies and procedures, facilitate information sharing internally and with the System, design program metrics, and sufficiently train Board and program staff. The Board has many existing information security policies and other documents that support such an effort, including its Continuity of Operations Plan, *Information Classification and Handling Standard*, and Program for Security of FOMC Information. These policies and other documents may provide a useful starting point in developing a formal itemization of the Board's most critical assets.

Recommendation

We recommend that the COO, in conjunction with relevant Board and System stakeholders,

1. Define the Board's critical and unique assets and assess the risks to those assets.

Management Response

In response to our draft report, the COO concurred with the finding and recommendation. The Board plans to compile a listing of critical assets and information and assess the risks associated with the assets and information. The Board plans to address this recommendation by the first quarter of 2027.

OIG Comment

The actions described by the COO appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 2: The Board Should Centralize Its Enterprise IRM Activities

The Board lacks a centralized IRM program to proactively manage insider risks at an enterprise level, whereas leading practices state that organizations should establish centralized program governance. The Board's four programs developed independently as a result of their specific responsibilities. However, this fragmented approach could degrade the agency's operational effectiveness. The third-party vendor retained by the Board in November 2024 also identified a lack of centralized IRM program and leadership as an issue for the Board.

The Board Lacks a Centralized Program to Manage Insider Risks

The Board has no centralized governance or single designated official who oversees the activities of its four programs, and the agency has not integrated IRM activities with its maturing enterprise risk management efforts. Further, the Board does not proactively or effectively identify and manage insider risks, as indicated by the lack of alignment with leading practices for designing and operating IRM programs, the maturity gap between the Board's IRM activities and a peer federal financial regulatory agency's program, and the Board's handling of recent insider risk incidents.[17] As a result, the nation's central bank lacks an enterprisewide view of its insider risk landscape.

Multiple Board officials acknowledged that the agency needs a centralized governance structure for managing Boardwide insider risks. The Board operates four programs that focus on information security incidents for each program's specific responsibilities. While the purposes of these programs overlap, the programs operate mostly independently, share little information, do not clarify leadership responsibilities for incidents that span multiple divisions or programs, and ultimately report to different stakeholders. This dispersed operating environment leads to fragmented efforts, unclear ownership of risks, and a lack of consistency or agreement among Board officials about the significance of events.[18]

Leading Practices Call for Centralized Program Governance

Leading IRM practices state that IRM programs should establish a centralized hub overseen by a single senior official. The hub should include stakeholders from a broad range of functional areas and have a dedicated budget, staffing, analytics, and technology assets. Our peer federal financial regulatory agency

[17] In addition to our findings, the RBOPS report of System IRM notes that the System lacks clear and formalized IRM governance and recommends a single Systemwide IRM program that can standardize basic IRM principles such as determining critical assets, defining categories of risk, and sharing information.

[18] Our management alert report related to the Board's offboarding process controls for records management will include findings and recommendations related to the Board's response to a possible information security incident involving the potential removal of FOMC and other sensitive Board information.

benchmark comparison follows this leading practice and has a centralized hub that receives information on any potential insider risk incident from across the enterprise, conducts an initial assessment to triage any immediate security concerns, and convenes relevant stakeholders to determine necessary actions when appropriate. Our 2019 report *Strengthening Organizational Governance* also highlights the importance of establishing communication expectations with the Board of Governors and appropriate committees. NITTF emphasizes that agencies have latitude to develop a program tailored to their unique mission, organization, culture, and threat landscape. Leading practices also state that a mature governance structure is essential to effectively develop, deploy, and manage an IRM program.

A Centralized Hub Could Better Manage Insider Risks at the Enterprise Level

Senior Board officials agreed that a hub would be more effective than the current four programs' approach, and an official explained that the programs had developed independently as a result of their specific authorizations. We previously made the Board aware of concerns regarding its decentralized IRM program. In 2016, we recommended that the Board establish an agencywide insider risk strategy for sensitive but unclassified Board information; however, the Board has yet to address that recommendation.[19] Recently, our *2025 Audit of the Board's Information Security Program* found the Board's overall information security program is not effective and, among other things, highlighted that the Board does not have an information security classification for CSI.[20]

Combining multiple programs with similar purposes, goals, and functions removes duplication and overlap and can result in more effective use of the Board's resources. The Board could leverage practices from each program. For example, IINS has access to classified intelligence threats to the Board, IT has tools and analytical capability to monitor activity on the Board's networks, S&R analyzes data on S&R information security incidents at the Board and Reserve Banks, and the FOMC Secretariat has detailed knowledge of the types of sensitive information the Board and FOMC handle and the effect of any incidents involving that information (figure 2).

[19] Office of Inspector General, *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016.

[20] Office of Inspector General, *2025 Audit of the Board's Information Security Program*, OIT Report 2025-IT-B-011R, October 31, 2025.

Figure 2. Example of Potential Stakeholders and Participants in a Comprehensive IRM Program

Source: OIG analysis.

Note: PSO is People, Strategy, and Operations; ERM is enterprise risk management.

Given the Board's role as the nation's central bank and the FOMC's role in setting monetary policy, the theft or loss of assets from the Board's essential systems, processes, and sensitive economic information has the potential to degrade the agency's operational effectiveness and potentially damage the U.S. economy. A centralized hub will better marshal expertise and resources from across Board divisions and can help the Board close gaps in its enterprise view of the insider risk landscape.

Recommendation

We recommend that the COO

2. Establish a centralized IRM program, or hub, to collect and analyze information from all agency sources to identify insider risks related to the Board's critical assets. The IRM program should initiate appropriate responses to resolve identified concerns including
    a. a senior official or oversight group accountable for overseeing the agency's IRM program.
    b. documented governance processes and structures in bylaws and committee charters.
    c. clear escalation expectations for communicating with the Board of Governors and appropriate committees.

d. members consisting of program stakeholders from a broad range of functional areas, including stakeholders with specialized disciplinary expertise, to strengthen insider risk processes.

e. a dedicated insider risk budget that provides for staffing, analytic, and technology assets necessary to maintain and improve effectiveness in fulfilling its objectives.

Management Response

In response to our draft report, the COO concurred with the finding and recommendation. The Board plans to establish a hub to collect and analyze information associated with potential insider risk events. The Board also plans to establish an executive steering committee to develop program governance, contribute and review program policies and procedures, and consider courses of action for identified insider risk events, as needed. The Board plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

The actions described by the COO appear to be responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 3: The Board Should Establish Procedures to Timely Share Relevant Insider Risk Information Internally and with the System

The Board lacks procedures for timely sharing pertinent information internally and with the System. Leading practices state that IRM programs should establish reporting guidelines to provide IRM program personnel regular and timely access to information necessary to identify, analyze, and resolve insider risks. Having separate Board programs has created information silos that prevent regular and automatic information sharing between Board divisions and the System. Consistently sharing information within the Board and with the System may prevent an insider incident and protect the Board's and System's functions.

The Board Lacks Consistent and Timely Information Sharing

The Board's four programs do not have procedures to routinely and timely share relevant insider risk information with each other and key Board and System stakeholders. For example, our 2026 foreign travel monitoring evaluation found that although the Board collects information related to employee travel, it does not have a process to internally share this information between relevant Board divisions to aid in identifying and addressing risks.[21] FOMC Secretariat officials told us it would be helpful to have more ready access to such travel information

THE BOARD DOES NOT MONITOR THE TRAVEL OF ALL EMPLOYEES WITH ACCESS TO SENSITIVE INFORMATION

Suspicious international travel, including frequent or unexplained trips of short duration, attempts to conceal international travel, or inconsistencies in reported international travel, could indicate activities associated with espionage.

Our 2026 foreign travel monitoring evaluation found that the Board requires international travel reporting for employees with a security clearance, which represents about 12 percent of the Board's workforce. However, international travel reporting is not required for those eligible to access sensitive Board information, such as sensitive FOMC information and CSI, which represents 39 percent and 56 percent of the Board workforce, respectively. Without requiring those with access to sensitive information to report personal international travel, the Board may not be aware of any potentially suspicious behaviors before travel or of potential threats employees may face while abroad.

[21] Our 2026 foreign travel monitoring evaluation details areas in which the Board can strengthen its international travel processes to minimize the risks presented to Board information and its employees while traveling abroad. See Office of Inspector General, *The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks*, OIG Report 2026-MO-B-009R, June 15, 2026.

to help restrict employee access to certain sensitive information during international travel and to provide context around any potential incidents that arise (see sidebar).

[redacted] Moreover, each of the programs produces an annual incident report to catalogue incidents, responses, or lessons learned, but no aggregation or analysis of those materials occurs at an enterprise level.

Regarding System information sharing, the various policies and procedures for the Board's four programs provide some details about how the Board may share information about potential information security incidents. However, none of these policies require periodic sharing of insider risk information with System stakeholders. [redacted] For example, after one employee left the Board subsequent to the identification of serious insider risk concerns, they were considered for positions at two Reserve Banks, met with the Reserve Bank president at one of those banks, and presented economic research at a third Reserve Bank.

We understand that the four Board programs may separately receive information about potential incidents from the System. The Board programs' siloed nature can further limit the Board's ability to maximize the agencywide IRM benefits of such information.

Leading Practices Call for Established Information Sharing Procedures

Leading practices state that IRM programs should direct components responsible for intelligence, security, human resources, and other relevant organizational components to establish reporting guidelines to provide IRM program personnel regular and timely access to information, such as intelligence and counterintelligence information, that is necessary to identify, analyze, and resolve insider risks. In addition, agencies should establish repeatable and sustainable processes for information sharing. Agencies should also periodically review IRM program information sources and past insider inquiries to assess the relevance and utility of the sources of information and insider risk indicators. The peer federal financial regulatory agency we benchmarked against established information access and sharing procedures to facilitate the hub's IRM processing and analysis.

Consistently Sharing Information May Prevent Insider Risks

A senior Board official agreed that having separate Board programs has created information silos that prevent regular and automatic information sharing. The absence of a hub with automated information collection could prevent timely risk detection and proactively addressing patterns of behavior that span

multiple divisions or information types, which may result in the loss of critical information, compromised systems, and threats to the physical safety of employees.

Because the Board and System typically protect the same sensitive information, consistently sharing insider risk information between the Board and the System may help prevent an insider incident and protect Board and System functions. A centralized hub could make use of information and expertise from the Division of IT, FOMC Secretariat, IINS, S&R, and other Board divisions to address risks to the Board holistically. For example, a centralized hub could ensure that Board staff responsible for monitoring suspicious employee IT activity also had access to employee travel information, allowing for a more holistic insight into behavior patterns. Further, a centralized hub could direct People, Strategy, and Operations; Records Management; Board Ethics; and other functions to automatically share information that may help timely prevent, identify, and mitigate insider risks.

Recommendations

In establishing a centralized IRM hub, as recommended above, we recommend that the COO

3. Establish information sharing procedures between Board divisions and the centralized hub that
    a. direct components responsible for intelligence, security, human resources, and other relevant areas to establish reporting guidelines to provide IRM personnel regular and timely access to necessary information.
    b. direct relevant Board components to establish automatic sharing of information, or repeatable and sustainable processes for sharing necessary information to identify, analyze, and resolve insider risks.
    c. require a periodic review of IRM program information sources and past insider risk inquiries to assess the relevance and utility of the sources of information and indicators.
    d. establish clear lines of reporting and collaboration with System stakeholders, including RBOPS, National IT, and Reserve Bank IRM programs.
4. Ensure the centralized hub has timely access, as permitted, to available federal intelligence and counterintelligence reporting information, such as analytic products pertaining to adversarial threats.

Management Response

In response to our draft report, the COO concurred with the finding and recommendations. Regarding recommendation 3, the Board plans to establish a hub and charter that accounts for appropriate information sharing and escalation procedures. The Board plans to address this recommendation by the fourth quarter of 2026.

Regarding recommendation 4, the Board's planned hub will include personnel from the Board's Federal Intelligence Coordination Office, which is part of IINS. These individuals, who are already involved in the IINS IRM program, will have access to federal intelligence and counterintelligence reporting information. The Board plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

The actions described by the COO appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 4: The Board Should Establish Enterprisewide Insider Risk Policies and Procedures

The Board lacks or has inconsistent IRM policies and procedures, referral processes, program metrics, and program-activity reporting. We determined this is a result of the Board's siloed approach to IRM activities. Leading practices state that IRM programs should develop consistent and comprehensive IRM governance processes, policies, and procedures. In addition, the peer federal financial regulatory agency we benchmarked had more mature policies and procedures than the Board. Enhancing these processes and policies as part of an enterprisewide IRM program will help the Board to consistently manage insider risks and refer related incidents to the appropriate law enforcement authorities.

The Board Lacks Comprehensive Policies and Procedures to Consistently Manage Insider Risks

In addition to lacking a centralized hub, the Board does not have a singular policy for insider risks to classified and unclassified information that establishes consistent program procedures and civil liberty protections.

A peer federal financial regulatory agency established a standard operating procedure, governance charter, and implementation plan for its IRM program. The peer agency documented how it ensures that it conducts its IRM activities in accordance with applicable laws, policy, and guidelines, including whistleblower protection, civil liberties and privacy protections, and records retention schedules. Leading practices state that IRM programs should establish policies and procedures for centrally managed inquiry and response actions, including consulting legal and privacy officials, developing consistent due process and fairness procedures for disciplinary actions, developing guidelines for retention of records, establishing oversight mechanisms, and documenting governance processes.

The Board Has Inconsistent Guidelines for Referrals to the OIG and Other Law Enforcement

IINS has clear reportable thresholds for referring potential insider risk incidents to the OIG for criminal cases or to the FBI for espionage concerns. However, the other three Board programs, which cover unclassified information, do not have uniform guidance for referring incidents or risks to the OIG or outside entities. Further, existing procedures that provide the OIG's law enforcement officers with information about an incident are not always followed. For example, the Division of IT's program identified an employee as having potentially significant information security violations after communicating plans to leave the Board. This issue was never brought to the Board's Core Response Group, which includes the OIG (see sidebar).

UNESCALATED INSIDER RISK INCIDENT

In 2022, after an employee notified the Board of their plan to separate from the Board, the Division of IT's program alerted the employee's division that the employee had triggered over 8,000 data loss prevention alerts and uploaded 45 gigabytes of data to an unsecure cloud service in a little over a month. After Board IT raised these concerns, the activity continued, including emailing files to various recipients in China.

We were subsequently informed that the Division of IT, the Legal Division, Records Management, and the employee's division met to address the issue. The incident concluded with no action taken because the employee's division determined that the employee was conducting routine work. The Board did not convene its Core Response Group to further assess the matter.

In addition, the Board has three separate forms for Board staff to report potential information security incidents, depending on the type of data and the program, but lacks a centralized method for personnel to report a potential insider risk concern or incident. RBOPS's report of System IRM programs also found a lack of standardized law enforcement referral guidance across Reserve Banks as well as a lack of a central reporting mechanism for potential insider risk incidents.

Leading practices state that IRM programs should establish close coordination between the IRM program, general counsel, and law enforcement components with investigative authorities, and should establish thresholds for referrals to outside investigative authorities, such as to the FBI's counterintelligence division. A peer federal financial regulatory agency also includes the OIG in its IRM hub to enable seamless referrals for matters that may require law enforcement action. Further, leading practices state that agencies should establish an internal reporting method accessible to all employees.

The Board Has Inconsistent Program Metrics and Reporting

The Board's multiple programs either lack or have inconsistent metrics for achieving program goals and processes for reporting program activity. Additionally, the Board's three unclassified programs do not have a process to follow up and gather information about the resolution of an action. [redacted]

Leading practices state that IRM programs should develop criteria for anomalous behavior, create formal feedback loops, and develop guidelines and procedures for documenting each insider risk matter and response actions taken, including an incident repository to ensure that lessons learned are captured. Further, agencies should employ metrics to determine progress in achieving program objectives and to identify improvement opportunities. A peer federal financial regulatory agency established metrics for its IRM program and annually reports to senior leadership information on referrals, threats, accomplishments, and improvement goals.

Hub Policies and Procedures May Better Prevent or Detect Insider Risks

The lack of a centralized hub for Board IRM activities allowed the Board's four programs to develop independently, resulting in differing policies and procedures, referral processes, and program metrics. By not consolidating these activities into a centralized, coordinated hub, the Board risks inconsistent responses to similar risks, missed opportunities to detect enterprise patterns and trends, and inconsistent referrals of criminal activity to law enforcement. For example, in several of the insider risk incidents cited in this report, we believe that the Board should have conducted further inquiry before the employees' separation to determine whether these matters should have been referred to law enforcement. To accomplish this, a centralized hub could establish policies and procedures that leverage the expertise and resources of the Board to prevent or detect insider risks, strengthen the program over time by tracking performance metrics, consistently coordinate with the OIG and other law enforcement as appropriate, and take into consideration an employee's civil liberties.

Recommendations

In establishing a centralized IRM hub, as recommended above, we recommend that the COO

5. Establish policies and procedures for assessing and responding to insider risks involving both classified and unclassified information that
    a. centralize IRM program responses.
    b. balance the need for oversight reviews from legal and civil liberties and privacy officials.
    c. provide appropriate and consistent due process and fairness procedures for disciplinary actions.
    d. establish guidelines and procedures for records retention.
    e. establish clear thresholds for referrals to the OIG and external law enforcement officials.
6. Establish internal reporting sites for cleared and uncleared employees to refer potential concerns or incidents to the IRM program.
7. Define program objectives, including a strategic vision, and establish metrics to measure progress toward achieving them. When identifying areas requiring improvement for senior leadership, the program should
    a. use trends and baselines to establish criteria for anomalous behavior.
    b. create formal feedback loops from responders to the IRM program to keep it informed of matter resolution, request clarifying information, and aid deconfliction among internal and external stakeholders.
    c. develop guidelines and procedures for documenting each insider risk matter and response action taken, including an incident repository to capture lessons learned.

d. establish oversight mechanisms or procedures to ensure proper handling and use of records and data and to ensure that access to such records and data is restricted to program personnel.

Management Response

In response to our draft report, the COO concurred with the finding and recommendations. Regarding recommendation 5, the Board plans to develop insider risk policies and procedures with input from all stakeholders in the executive steering committee. The Board plans to address this recommendation by the fourth quarter of 2026.

Regarding recommendation 6, the Board plans to enhance existing IINS tools and procedures for reporting an insider threat. IINS plans to enhance reporting capability, communicate this resource to the workforce, and develop anonymous means for reporting insider risks. The Board plans to address this recommendation by the fourth quarter of 2026.

Regarding recommendation 7, IINS plans to develop metrics as the program evolves its regular monitoring as part of its trend analysis, which may be dependent on the implementation of a case management system. The Board plans to address this recommendation by the fourth quarter of 2027.

OIG Comment

The actions described by the COO appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 5: The Board Should Require IRM Training for All Board and IRM Personnel

The Board does not have consistent training requirements, including formal training in counterintelligence and security principles, across its four programs. Only IINS requires specific training in applicable laws and regulations regarding records retention, civil liberties, and privacy for its program staff. In addition, the Board only requires staff with security clearances to take insider risk training.

Leading practices state that IRM programs should designate staff to serve as IRM analysts and provide required and continuing training in counterintelligence and security principles, techniques, and tools, including behavioral science perspectives. Further, programs should require program staff to be fully trained in applicable laws and regulations regarding records retention, civil liberties, and privacy. In addition, leading practices indicate that all agency staff should take insider risk training. A peer federal financial regulatory agency requires training for dedicated IRM hub staff, which includes training for counterintelligence, insider risk detection and analysis, and privacy and civil liberties.

The lack of a centralized IRM hub for classified and unclassified information has led to these four programs having separate training expectations and policies. Further, in the absence of a centralized IRM program, there is no clear, single advocate to press for change in requiring all Board employees to receive insider risk training.

Because IRM programs depend on collaboration among multiple offices and the synthesis of many disparate information sources, personnel associated with these efforts need fundamental knowledge across a wide range of disciplines. Without proper training, the Board cannot ensure that all relevant IRM staff possess the basic levels of understanding needed to perform their duties appropriately. Further, a highly aware workforce is key to early detection and prevention of malicious insider threat conduct. Therefore, training uncleared staff on potential insider risk indicators and threats will help them to be vigilant in detecting and reporting potential concerns to the appropriate personnel.

Recommendations

When establishing a consolidated hub, we recommend that the COO

8. Designate staff to serve as insider risk analysts and provide them with relevant training to develop IRM skills and competencies, including
    a. requiring all IRM program personnel to have some level of formal training in counterintelligence and security principles, techniques, and tools, including behavioral science perspectives and expertise.
    b. requiring all IRM program personnel to be fully trained in applicable laws and regulations regarding records retention, civil liberties, and privacy laws.
    c. providing continuing education and training in appropriate fields and disciplines.

9. Require that all Board personnel take IRM training annually.

Management Response

In response to our draft report, the COO concurred with the finding and recommendations. Regarding recommendation 8, the Board plans to ensure that analysts contributing to the IRM program will be identified and receive appropriate training. The Board plans to address this recommendation by the fourth quarter of 2026.

Regarding recommendation 9, the Board plans to develop and require insider risk training for all Board personnel. The Board plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

The actions described by the COO appear to be responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Appendix A: Scope and Methodology

Our objective was to assess the design and effectiveness of the Board's IRM activities. To accomplish our objective, we assessed whether the Board's IRM activities are consistent with leading practices. Our scope covered the Board's governance and management of activities to detect, deter, and mitigate insider risks, including the Board's and the System's coordination on incident response and reporting. Our scope did not include assessing IRM activities conducted by the Reserve Banks or System entities.

To accomplish our objective, we first identified the Board activities and programs related to responding to or managing insider risks, which consisted of programs in the Division of IT, the FOMC Secretariat, IINS, and S&R.

We then identified leading practices from a broad range of sources, including those from the U.S. government, academia, and the private sector, and aggregated them into six themes: (1) governance and organizational design, (2) policies and procedures, (3) information access, (4) training, (5) records retention, and (6) information processing and analysis. For each theme, we focused on leading practices to test the design and effectiveness of the governance and management of the Board's programs. The sources consisted of

- National Insider Threat Task Force, *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*, 2024
- National Insider Threat Task Force, *Protect Your Organization from the Inside Out: Government Best Practices*, 2016
- National Insider Threat Task Force, *Insider Threat Program Maturity Framework*, November 1, 2018
- Office of Inspector General, *Strengthening Organizational Governance*, OIG Insights, February 14, 2019
- Securities Industry and Financial Markets Association, *Insider Threat Best Practices Guide*, 3rd Edition, July 2024
- Software Engineering Institute, *Common Sense Guide to Mitigating Insider Threats*, Carnegie Mellon University, 2022

We also benchmarked with a peer federal financial regulatory agency's IRM program to understand its practices for managing relevant risks and compare the Board's current processes. That benchmarking included multiple meetings with the peer agency's program leader and reviewing documentation related to their program.

Finally, to identify any gaps in the Board's IRM activities, including incident detection, handling, and reporting, we reviewed selected potential insider risk incidents at the Board and the Division of IT, FOMC Secretariat, and IINS incident reporting. We interviewed officials and staff from the following Board divisions: Management and Financial Services, Financial Stability, International Finance, IT, Legal, Monetary Affairs, RBOPS, S&R, and the Office of the Chief Operating Officer. We also interviewed multiple System staff.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. We conducted this work from March 2025 to March 2026.

Appendix B: Management Response

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

OFFICE OF THE
CHIEF OPERATING OFFICER

June 30, 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 review and comment on the Office of Inspector General's (OIG) draft report titled *The Board Needs a More Robust Insider Risk Management Program*. We appreciate the OIG's effort to develop the report and recommendations to further strengthen the Board's Insider Risk Management (IRM) program, processes, and activities.

We are proud of the work accomplished by our Intelligence, Insider Risk, and National Security Programs (IINS) team. We realize we have additional work to enhance the IRM program's ability to more effectively identify and manage risks to the Board's information and assets.

We have reviewed the report and concur with the five findings and nine recommendations. We have already begun work that we believe is responsive to your findings and recommendations. Our responses for each recommendation are included below.

We value your objective and independent viewpoints, and appreciate the professionalism demonstrated by all OIG personnel throughout this audit and your efforts to understand our IRM program, processes, and activities. We look forward to continued work with your office in the future.

Regards,

Winona Varnon

Winona H. Varnon

cc:

Jeff Reidel
Rendell Jones
Trevor Reeve
Randall Guynn
Susan Foley
Chip Young
Nelly Ramdass
Matthew Luecke
Tannaz Haddadi
Amy Kelley
Kelly Gibbs
Melissa Catterall
Leah Middleton
Linda Comilang

Response to recommendations presented in the Draft OIG Report,

"The Board Needs a More Robust Insider Risk Management Program"

Finding 1: The Board Should Identify and Assess Its Critical Assets

Recommendation 1: Define the Board's critical and unique assets and assess the risks to those assets.

Management Response:
We concur with this recommendation and will compile a listing of critical assets and information and assess the risk associated with each. Target Date: CY27Q1.

Finding 2: The Board Should Centralize Its Enterprise IRM Activities

Recommendation 2: Establish a centralized IRM program, or hub, to collect and analyze information from all agency sources to identify insider risks related to the Board's critical assets. The IRM program should initiate appropriate responses to resolve identified concerns including:

a. a senior official or oversight group accountable for overseeing the agency's IRM program.
b. documented governance processes and structures in bylaws and committee charters.
c. clear escalation expectations for communicating with the Board of Governors and appropriate committees.
d. members comprised of program stakeholders from a broad range of functional areas, including stakeholders with specialized disciplinary expertise, to strengthen insider risk processes.
e. a dedicated insider risk budget that provides for staffing, analytic, and technology assets necessary to maintain and improve effectiveness in fulfilling its objectives.

Management Response:
We concur with this recommendation. The Insider Risk Management Program Office (IRMPO) under the Chief Operating Officer will establish a hub to collect and analyze information associated with potential insider risk events. Additionally, an Executive Steering Committee will be established to develop program governance, contribute and review program policies and procedures, and consider courses of action for identified insider risk events, as needed. Target Date CY26Q4.

Finding 3: The Board Should Establish Procedures to Timely Share Relevant Insider Risk Information Internally and with the System

Recommendation 3: Establish information sharing procedures between Board divisions and the centralized hub that:

a. direct components responsible for intelligence, security, human resources, and other relevant areas to establish reporting guidelines to provide IRM personnel regular and timely access to necessary information.

b. direct relevant Board components to establish automatic sharing of information, or repeatable and sustainable processes for sharing necessary information to identify, analyze, and resolve insider risks.

c. require periodic review of IRM program information sources and past insider risk inquiries to assess the relevance and utility of the sources of information and indicators.

d. establish clear lines of reporting and collaboration with System stakeholders, including RBOPS, National IT, and Reserve Bank IRM programs.

Management Response:
We concur with this finding. The IRMPO will establish a hub and charter that accounts for appropriate information sharing and escalation procedures. Target Date: CY26Q4.

Recommendation 4: Ensure the centralized hub has timely access, as permitted, to available federal intelligence and counterintelligence reporting information, such as analytic products pertaining to adversarial threats.

Management Response:
We concur with this finding. The hub will include personnel from the Federal Intelligence Coordination Office, which is part of IINS. These individuals, already involved in the Insider Threat Program, have access to this reporting information. Target Date: CY26Q4.

Finding 4: The Board Should Establish Enterprisewide Insider Risk Policies and Procedures

Recommendation 5: Establish policies and procedures for assessing and responding to insider risks involving both classified and unclassified information that

a. centralize IRM program responses.

b. balance the need for oversight reviews from legal and civil liberties and privacy officials.

c. provide appropriate and consistent due process and fairness procedures for disciplinary actions.

d. establish guidelines and procedures for records retention.

e. establish clear thresholds for referrals to the OIG and external law enforcement officials.

Management Response:
We concur with this finding. The IRMPO, with input from all stakeholders and the ESC, will develop insider risk policies and procedures. Target Date: CY26Q4.

Recommendation 6: Establish internal reporting sites for cleared and uncleared employees to refer potential concerns or incidents to the IRM program.

Management Response:
We concur with this finding. IINS has a tool and procedures for reporting an insider threat. IINS will enhance reporting capability, communicate this resource to the workforce, and develop an anonymous means for reporting. Target Date: CY26Q4.

Recommendation 7: Define program objectives, including a strategic vision, and establish metrics to measure progress toward achieving them. When identifying areas requiring improvement for senior leadership, the program should

a. use trends and baselines to establish criteria for anomalous behavior.

b. create formal feedback loops from responders to the IRM program to keep it informed of matter resolution, request clarifying information, and aid deconfliction among internal and external stakeholders.

c. develop guidelines and procedures for documenting each insider risk matter and response action taken, including an incident repository to capture lessons learned.

d. establish oversight mechanisms or procedures to ensure proper handling and use of records and data and to ensure that access to such records and data is restricted to program personnel.

Management Response
We concur with this recommendation. IINS will develop metrics as the program evolves monitoring regularly as part of the trend analysis. Metrics for reporting on the program's success may be dependent upon implementation of a case management system. Target Date: CY27Q4.

Finding 5: The Board Should Require IRM Training for All Board and IRM Personnel

Recommendation 8: Designate staff to serve as insider risk analysts and provide them with relevant training to develop IRM skills and competencies, including

a. requiring all IRM program personnel to have some level of formal training in counterintelligence and security principles, techniques, and tools, including behavioral science perspectives and expertise.

b. requiring all IRM program personnel to be fully trained in applicable laws and regulations regarding record retention, civil liberties, and privacy laws.

c. providing continuing education and training in appropriate fields and disciplines.

Management Response:
We concur with this recommendation. Analysts contributing to the insider risk management program will be identified and receive appropriate training. Target Date: CY26Q4.

Recommendation 9: Require that all Board personnel take IRM training annually.

Management Response:
We concur with this recommendation. Insider Risk training will be developed and required for all Board personnel. Target Date: CY26Q4.

Abbreviations

COO	chief operating officer
CSI	confidential supervisory information
FBI	Federal Bureau of Investigation
FOMC	Federal Open Market Committee
IINS	Intelligence, Insider Risk, and National Security Programs
IRM	insider risk management
IT	information technology
National IT	Federal Reserve National Information Technology
NITTF	National Insider Threat Task Force
RBOPS	Division of Reserve Bank Operations and Payment Systems
S&R	Division of Supervision and Regulation

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

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 Information

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