Evaluation Report
2025-MO-B-010
August 20, 2025

Board of Governors of the Federal Reserve System

The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program

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

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

Executive Summary, 2025-MO-B-010, August 20, 2025

The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program

Findings

The Board of Governors of the Federal Reserve System's physical security program, while generally effective, can be strengthened in multiple foundational respects.

Specifically, the Board's Law Enforcement Unit (LEU) executes the physical security program without formally delegated decisionmaking authority and without established physical security standards. The lack of these foundational components complicates the resolution of physical security concerns, particularly when the LEU coordinates with the Board's Facility Services section on design, construction, or renovation matters. The Board also lacks a formal process for addressing identified security risks and documenting risk mitigation decisions. Further, the Board does not have clear processes for managing third-party access cards typically provided to staff assigned to leased workspaces. Without a process to collect and deactivate these access cards from employees and contractors who leave the agency, the Board faces potential building access vulnerabilities that should be addressed.

Finally, we determined that the LEU's Technical Security Bureau does not have policies and procedures or performance objectives that guide most of its physical security functions and responsibilities. The lack of these foundational materials impedes the Board's ability to assess and monitor program effectiveness.

Recommendations

Our report contains six recommendations designed to enhance aspects of the Board's physical security program, including clarifying the LEU's authority and documenting processes. In its response to our draft report, the Board concurs with our recommendations and outlines actions to address each recommendation. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We initiated this evaluation in June 2024 to assess whether the Board has an effective oversight structure to manage its physical security program and whether selected security measures in Board spaces are effective.

Background

The LEU provides a safe and secure environment for Board staff and visitors at each of the Board's six properties by protecting infrastructure and critical facilities, mitigating or eliminating security risks, and responding to incidents. The LEU's Technical Security Bureau manages the technical components of the Board's physical security program, including access controls and surveillance equipment, among other duties.

Recommendations, 2025-MO-B-010, August 20, 2025

The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program

Finding 1: The Board Should Clarify Authorities and Establish Standards and a Decisionmaking Process for Physical Security Matters

Number	Recommendation	Responsible office
1	Clarify and document the Division of Management's formal delegation of authority to the LEU for Board physical security decisions.	Division of Management
2	Establish and document physical security standards for the agency that include a risk-based decisionmaking framework to a. raise and resolve physical security considerations and concerns. b. document physical security decisions, including describing the rationale for any deviations from physical security standards.	Division of Management

Finding 2: The Board Should Develop a Process to Collect, Deactivate, and Reconcile Third-Party Access Cards

Number	Recommendation	Responsible office
3	Assign responsibility for managing third-party access cards for Board-leased spaces.	Division of Management
4	Ensure that the responsible group develops and implements a process to a. collect and deactivate third-party access cards from offboarded Board personnel. b. periodically reconcile third-party access card rights against human resources' list of active Board employees and contractors.	Division of Management

Finding 3: The LEU Should Document the TSB's Responsibilities and Processes

Number	Recommendation	Responsible office
5	Establish a policy that defines the TSB's responsibilities and the standard operating procedures needed to fulfill those responsibilities.	Law Enforcement Unit

Finding 4: The LEU Should Further Establish Objectives for the TSB and Monitor Its Performance

Number	Recommendation	Responsible office
6	Develop and document a. measurable performance objectives for the TSB's responsibilities. b. a monitoring process to assess the TSB's progress toward achieving those objectives.	Law Enforcement Unit

Contents

Introduction

Objective

We assessed whether the Board of Governors of the Federal Reserve System has an effective oversight structure to manage its physical security program and whether selected security measures in Board spaces are effective. Our evaluation covered several aspects of the Board's physical security program, including oversight and governance, access controls, surveillance, vulnerability assessments, and management of third-party access cards[1] for leased spaces. Appendix A provides additional details about our scope and methodology.

Background

The Board owns four buildings—Marriner S. Eccles, William McChesney Martin Jr., New York Avenue, and 1951 Constitution Avenue—and leases space in two others. The Board's Law Enforcement Unit (LEU), which is part of the Division of Management, provides a safe and secure environment for staff and visitors in the four buildings it owns and in its leased spaces by protecting infrastructure and critical facilities, mitigating or eliminating security risks, and responding to incidents.

The Board's chief operating officer has delegated authority to the director of the Division of Management to manage the agency's physical security. A chief manages the LEU and reports to the director. The LEU consists of four bureaus. The Operations Bureau provides a physical security presence and operates a variety of physical security countermeasures to protect Board property and personnel; the Operations Support Bureau manages supplies and administrative activities; the Training Bureau develops training for both LEU officers and civilian staff; and the Technical Security Bureau (TSB) manages the technical components of the Board's physical security program, including access controls and surveillance equipment, among other duties.

The Board's Physical Security Structure

The Board's physical security program consists of access control systems, surveillance monitoring, security posts, reinforced entry points, and other physical and technical security countermeasures. The Board issues personal identity verification (PIV) cards to allow personnel access to its owned buildings and leased workspaces. The lessor issues third-party access cards to Board staff working in leased spaces.

As part of the physical security program, the TSB coordinates with the U.S. Department of Homeland Security (DHS) to conduct risk assessments to determine the level of protection needed for Board-owned and -leased spaces. The Board's TSB and Facility Services coordinate on the design and installation of security countermeasures for Board construction and renovation projects.

[1] Third-party access cards provide access to certain areas of leased spaces, including building common areas and amenities as well as elevators to Board-occupied floors, but do not allow entry to Board-leased workspaces.

Technical Security Bureau. The TSB has eight staff, including locksmiths, security analysts, specialists, and technicians, and is led by a supervisor who reports to the assistant chief of the LEU. The TSB reviews physical security designs, implements, and manages the Board's physical and technical security systems and programs. Physical security countermeasures under the TSB's oversight include surveillance cameras, magnetometers, x-ray scanning machines, PIV card readers, and physical keys and locks (see table).

Table. The TSB's Security Functions and Responsibilities

TSB function	Responsibilities
The **physical security** function includes installing and maintaining the Board's security equipment, reviewing physical security designs, and coordinating vulnerability assessments of agency buildings.	**PIV cards:** (1) issue and maintain PIV cards and PIV card readers and (2) manage data entry in the access control system to assign, track, update, and revoke PIV card access permissions **Surveillance cameras:** (3) manage the installation and maintenance of surveillance cameras and video storage devices **Locks and keys:** (4) distribute and maintain physical keys and (5) install and maintain locks for owned and leased spaces, including the sensitive compartmented information facility **Screening equipment and doors:** (6) coordinate with vendors for installing and maintaining x-ray machines, magnetometers, turnstiles, and revolving doors **Design review:** (7) coordinate with Facility Services to review and provide physical security feedback about construction and renovation designs **Vulnerability assessments:** (8) coordinate with DHS to perform periodic vulnerability assessments of owned and leased spaces to identify and address physical security risks **Research:** (9) identify and assess new technologies to improve operational efficiencies and physical security
The **technical security** function includes managing the Board's electronic and signals countermeasures.	**External/government security groups:** (10) submit annual reporting requirements to the Interagency Security Committee and (11) serve as the Board's Technical Surveillance Countermeasures[a] program manager in the Intelligence Community **Internal signal countermeasures:** (12) manage the in-place monitoring system program[b] and (13) coordinate inspections of sensitive locations, such as the sensitive compartmented information facility

Source: OIG analysis.

[a] The Office of the Director of National Intelligence states that technical surveillance countermeasures seek to detect and nullify a wide variety of technologies used to gain unauthorized access to restricted or otherwise sensitive information.

[b] This program continuously monitors radio frequencies at the Board to help detect abnormal frequencies.

Facility Services. Facility Services, within the Division of Management, addresses space planning, engineering, design, construction, operation, and maintenance of Board facilities. As part of these responsibilities, Facility Services oversees both small- and large-scale Board renovation and construction projects and coordinates these efforts with agency stakeholders, including the LEU. Facility Services consults with external vendors and the TSB about the design and implementation of specific physical security countermeasures during construction and renovation projects, such as determining the locations for PIV card readers.

In addition, Facility Services manages the access rights, distribution, and tracking of third-party access cards for Board-leased spaces. Board personnel requiring access to leased space submit a request to the lessor and Facility Services, the lessor issues an access card, and Facility Services adds access rights to Board-occupied floors.[2]

Policies and Guidance

Several policies and guidance documents are applicable to the Board's physical security program.

LEU *General Orders.* The LEU maintains a manual that establishes rules, regulations, procedures, and guidance for LEU personnel about topics such as staffing posts, screening visitors, and responding to threats.

Facility Standards Manual. Facility Services maintains this manual, which establishes design standards and criteria for new Board buildings and for renovations, alterations, and repairs to existing Board space. The manual states that Interagency Security Committee (ISC) standards apply to new Board construction and major modernization projects. The manual notes that the LEU will provide further direction about physical security as needed.

ISC Standards. ISC standards are a set of security standards applicable to all federally owned or leased buildings. The standards outline recommended security countermeasures and guidance for determining a building's facility security level (FSL).[3] ISC standards include a framework to help federal agencies determine the appropriate countermeasures for a building's FSL, as well as a process for accepting and documenting risk when recommended security measures cannot be met. While the Board is not required to follow ISC standards, both the TSB and Facility Services voluntarily use ISC standards for design, construction, and physical security.

[2] Facility Services uses the lessor's third-party access card management system to add access rights to one of the Board-leased buildings and coordinates with the Board's second lessor to add access to its building.

[3] The FSL is a categorization (levels I, II, III, IV, and V) based on the analysis of several security-related factors, such as building size, number of staff, and mission criticality, and determines the level of protection needed and recommended countermeasures for a building.

Finding 1: The Board Should Clarify Authorities and Establish Standards and a Decisionmaking Process for Physical Security Matters

The Board has not established authorities, standards, or a decisionmaking process for the physical security program. The LEU executes the Board's physical security program, but the director of the Division of Management has not further delegated that authority formally to the LEU. Regarding standards, the TSB and Facility Services separately referenced the use of ISC standards for the design of Board buildings, but neither party has documented the extent to which these standards should be followed and applied or the process for assessing and identifying the need for exceptions to the standards. The Board also does not have a formal process to resolve physical security concerns and document physical security decisions when the LEU coordinates with Facility Services on the design and construction of new and renovated Board spaces.

The U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states that management should define and assign responsibilities and delegate authority to achieve objectives. In addition, management should document policies that outline each unit's responsibilities for achieving process objectives, managing risks, and ensuring controls are properly designed, implemented, and functioning effectively. Further, ISC standards require agencies to assess risks, document risk acceptance decisions, and justify any deviations from baseline security requirements to ensure transparency and accountability.

During a policy review in 2023, the LEU removed a general order that broadly defined the TSB's purpose as providing technical security expertise in support of the LEU's day-to-day operations. This general order did not define the TSB's authority or role in the design of physical security measures, including how the TSB should coordinate with Facility Services about physical security issues related to construction and renovation projects. While we were informed of regular meetings between the LEU and Facility Services to discuss (1) current physical security concerns about construction and renovation projects, (2) establishing physical security standards, and (3) construction project updates for senior leaders, we did not see any documentation showing physical security considerations or concerns being addressed and resolved, standards being agreed upon, or final physical security decisions from those meetings.

The lack of clear delegations of formal authority, established standards, and a defined decisionmaking process for the Board's physical security program has led to some confusion or disagreement between the TSB and Facility Services, and prevents the objective, standardized assessment and mitigation of physical security risks during the design and construction of its spaces. We believe that documenting the LEU's formal delegation of authority for Board physical security matters, establishing physical security standards, and implementing a risk-based decisionmaking framework may establish a better foundation to consider risks when making physical security decisions.

Recommendations

We recommend that the director of the Division of Management

1. Clarify and document the Division of Management's formal delegation of authority to the LEU for Board physical security decisions.
2. Establish and document physical security standards for the agency that include a risk-based decisionmaking framework to
    a. raise and resolve physical security considerations and concerns.
    b. document physical security decisions, including describing the rationale for any deviations from physical security standards.

Management Response

In response to our draft report, the acting director of the Division of Management concurs with our recommendations. Regarding recommendation 1, the response states that the Board will update the appropriate delegations of authority to the LEU by the fourth quarter of 2025.

Regarding recommendation 2, the response states that the LEU will develop a physical security policy that will (1) formalize the standards the Board currently follows, (2) include a new risk-based decisionmaking framework for security considerations and concerns, and (3) address the rationale for decisions and deviations from the standards. In addition, the LEU will expand its physical security standard operating procedures (SOPs) to document how the new decisionmaking framework is used and how program personnel handle and document all decisions. The Board estimates it will complete these efforts by the fourth quarter of 2026.

OIG Comment

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

Finding 2: The Board Should Develop a Process to Collect, Deactivate, and Reconcile Third-Party Access Cards

The Board does not have a process to collect, deactivate, and reconcile third-party access cards used in leased spaces. The LEU was managing third-party access cards, including collecting cards in certain circumstances, but had no written guidance for its processes and informally transitioned that responsibility to Facility Services in 2023. Facility Services has since implemented an SOP and a process workflow for adding access rights to third-party access cards, distributing the cards to Board employees and contractors, and tracking the issuance of the cards; however, Facility Services does not collect, deactivate, and reconcile the access cards of separating employees or contractors.

GAO's *Standards for Internal Control in the Federal Government* states that management should define and assign responsibilities and delegate authority to achieve objectives. In addition, management should perform ongoing monitoring to ensure operating effectiveness of the internal control system. GAO states that *ongoing monitoring* includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions.

Although Facility Services manages third-party access cards, the responsibility has not been formally assigned. The transition from the LEU to Facility Services was informal; we were informed by a Facility Services official that this decision was not escalated to the director of the Division of Management and that Facility Services envisioned that transition to be temporary. In addition, the Board's human resources section (People, Strategy and Operations) does not notify Facility Services of separating Board employees and contractors.

While third-party access cards do not grant direct access into Board-leased spaces, the lack of a deactivation and reconciliation process increases the risk of unauthorized access. Assigning responsibility and creating a process to collect, deactivate, and reconcile the inventory of issued third-party access cards will help to ensure that only Board employees and contractors have access to Board-occupied floors in leased spaces.

Recommendations

We recommend that the director of the Division of Management

3. Assign responsibility for managing third-party access cards for Board-leased spaces.
4. Ensure that the responsible group develops and implements a process to
    a. collect and deactivate third-party access cards from offboarded Board personnel.
    b. periodically reconcile third-party access card rights against human resources' list of active Board employees and contractors.

Management Response

In response to our draft report, the acting director of the Division of Management concurs with our recommendations. Regarding recommendation 3, the response states that the LEU will assume full responsibility of the third-party access card process by the first quarter of 2026.

Regarding recommendation 4, the response states that by the first quarter of 2026, the LEU will update the third-party access card process to include the collection and deactivation of these cards for offboarded Board personnel and will establish a periodic schedule to compare a list of active third-party access card holders against a list of active Board employees and contractors.

OIG Comment

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

Finding 3: The LEU Should Document the TSB's Responsibilities and Processes

The TSB has policies or SOPs to guide its actions for 3 of its 13 responsibilities related to certain areas of its management of the surveillance cameras, PIV cards, and physical keys.[4] The remaining 10 responsibilities have no formal guidance and include, among other items, reviewing physical security designs, coordinating with DHS to conduct vulnerability assessments of Board facilities, and inspecting the Board's sensitive compartmented information facility and other sensitive areas. In the absence of policies and SOPs, the TSB has developed some undocumented procedures. For example, the TSB reconciles the Board's access control database against the Board's internal personnel system and other external government systems of record on a weekly basis, but this reconciliation process is not documented and there is no guidance for how to conduct this reconciliation and which systems to include in it.

GAO's *Standards for Internal Control in the Federal Government* states that management should document policies for operational processes that outline each unit's responsibilities for achieving process objectives, managing risks, and ensuring controls are properly designed and implemented.

A previous LEU general order established the TSB's purpose and outlined roles and responsibilities for the TSB manager and locksmith positions, but did not include details or additional guidance for the remaining TSB positions and their responsibilities. An LEU official informed us that the general order was removed in December 2023 during a policy review because it was duplicative of information maintained in a broader set of LEU job descriptions, which included the TSB. The TSB supervisor informed us that the TSB intends to document responsibilities and associated processes, but we had not received these materials as of May 2025.

We believe documenting all the TSB's responsibilities and internal processes will help ensure consistency and repeatability for its duties, such as when performing reconciliations of the Board's access control database. Internal processes and SOPs can provide guidance for cross-training so that the TSB is better prepared for staffing disruptions or staff turnover that could affect the execution of their core functions. In addition, documentation will allow LEU leadership to better align the TSB with other LEU bureaus that maintain documentation for their operations.

Recommendation

We recommend that the chief of the LEU

5. Establish a policy that defines the TSB's responsibilities and the standard operating procedures needed to fulfill those responsibilities.

[4] The LEU finalized a key and lock policy in March 2025 that establishes procedures for requesting keys, changing locks, and locking sensitive areas.

Management Response

In response to our draft report, the acting director of the Division of Management concurs with our recommendation. The response states that the TSB has drafted an initial SOP fully documenting its responsibilities and processes and that the TSB anticipates implementing the SOP by the second quarter of 2026.

OIG Comment

The planned action described by the Board appears responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 4: The LEU Should Further Establish Objectives for the TSB and Monitor Its Performance

The LEU has not fully established TSB-specific performance objectives or a process to monitor program effectiveness. In a review of the 2025 LEU objectives, we noted just one performance objective related to a TSB responsibility. In addition, we noted six shared team goals that were communicated to the TSB by its leadership. We reviewed both the LEU's performance objective and the TSB-specific goals and found that they do not fully capture the TSB's functional areas and responsibilities.

GAO's *Standards for Internal Control in the Federal Government* states that management should define measurable objectives so that performance toward achieving those objectives can be assessed. In addition, management should compare actual performance to planned or expected results and analyze significant differences.

Senior LEU officials indicated that the TSB's primary role is to advance new technology for potential implementation, but they did not inform us of any performance goals for the remaining functions or responsibilities. We were informed that the TSB uses the Board's performance management system to track team performance on an individual employee basis; however, these individual goals do not address all the TSB's functions and do not provide comprehensive monitoring capabilities to assess the TSB's effectiveness.

The lack of measurable performance objectives prevented our team from fully assessing how each of the TSB's responsibilities helped achieve its overall goals. In addition, the lack of TSB performance objectives may hinder LEU management's ability to fully assess the program's performance and identify opportunities for future improvement. While we understand that the TSB manager assesses TSB employees as part of the Board's performance management system, establishing program-specific objectives will help ensure progress toward meeting the overall goals for the physical security program.

Recommendation

We recommend that the chief of the LEU

6. Develop and document
    a. measurable performance objectives for the TSB's responsibilities.
    b. a monitoring process to assess the TSB's progress toward achieving those objectives.

Management Response

In response to our draft report, the acting director of the Division of Management concurs with our recommendation. The response states that by the fourth quarter of 2025, the TSB will develop and

incorporate program- and employee-level objectives and measures that will be incorporated into the Board's performance management system. The response also states that by the fourth quarter of 2026, the TSB will develop a program-level monitoring process to annually assess the TSB's performance.

OIG Comment

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

Appendix A: Scope and Methodology

We initiated this evaluation in June 2024 to assess whether the Board has an effective oversight structure to manage its physical security program and whether selected security measures in Board spaces are effective. To accomplish our objective, we interviewed officials from the Board's LEU, including staff from the TSB, the Operations Bureau, and the Operations Support Bureau, as well as personnel from Facility Services. We reviewed relevant LEU *General Orders*, TSB position descriptions, and SOPs to understand roles and responsibilities. We also reviewed the *Facility Standards Manual*, ISC standards, and internal communications to assess how physical security measures are designed, implemented, and maintained. In addition, we identified applicable criteria, including GAO's *Standards for Internal Control in the Federal Government*.

We focused on several aspects of the Board's physical security program, including oversight and governance, access controls, surveillance, vulnerability assessments, and the management of third-party access cards for leased spaces. Our work included reviews of relevant documentation, system walkthroughs, and interviews with responsible staff to understand access control practices, key and card management, surveillance protocols, and the process for conducting and tracking vulnerability assessments. We also compared the Board's access control system against Board personnel records.

We conducted our fieldwork from October 2024 through June 2025. We performed this evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: Management Response

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

DIVISION OF MANAGEMENT

August 8, 2025

Mr. Michael VanHuysen
Associate Inspector General for Audits and Evaluations
Office of Inspector General
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's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program.* We appreciate the OIG's effort to develop the report and recommendations to further strengthen our physical security program.

We are proud of the work accomplished by our Law Enforcement Unit's (LEU) Technical Security Bureau (TSB). We realize we have additional work to improve our physical security program to better protect the Federal Reserve Board.

We have reviewed the report and concur with the four findings and six 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 security processes . We look forward to continued work with your office in the future.

Regards,

WINONA VARNON Digitally signed by WINONA VARNON Date: 2025.08.05 16:55:52 -04'00'

Winona H. Varnon

www.federalreserve.gov

cc:

Don Hayes
Al Dyson
Donna Butler
Kendra Gastright
Leah Middleton
Ryan Chu
Mike Bagley
Linda Comilang
Tim Ly
Tara Pelitere

Response to recommendations presented in the Draft OIG Report,

"The Board's Law Enforcement Unit Can Clarify Its Authority and Document Processes for Its Physical Security Program"

Finding 1: The Board Should Clarify Authorities and Establish Standards and a Decision-making Process for Physical Security Matters

Recommendation 1: Clarify and document the Division of Management's formal delegation of authority to the LEU for Board physical security decisions.

Management Response: We concur with the finding and recommendation. We are in the process of updating the Chief Operating Officer's Delegation of Authority to the Director, Division of Management and will ensure we update it to reflect the appropriate delegations to the LEU. We are targeting an implementation by Q4 2025.

Recommendation 2: Establish and document physical security standards for the agency that include a risk-based decision-making framework to

a. raise and resolve physical security considerations and concerns.

   Management Response: We concur with the finding and recommendation. LEU will develop a physical security policy to formalize the standards we currently follow and include a new risk-based decision-making framework for security considerations, concerns, and deviations. Additionally, we will expand our standard operating procedures (SOPs) for physical security to document how the program operates and how the risk-based decision-making framework is utilized for physical security considerations, concerns, and deviations. We are targeting an implementation by Q4 2026.

b. document physical security decisions, including describing the rationale for any deviations from physical security standards.

   Management Response: We concur with the finding and recommendation. In (a) above, we will address rationale for decisions and deviations from physical security standards. Additionally, physical security SOPs will describe how program personnel handle and document all decisions. We are targeting an implementation by Q4 2026.

Finding 2: The Board Should Develop a Process to Collect, Deactivate, and Reconcile Third-Party Access Cards

Recommendation 3: Assign responsibility for managing third-party access cards for Board-leased spaces.

Management Response: We concur with the finding and recommendation. Currently, the Facilities Services (FS) branch of the Division of Management oversees the third-party access card process. For centralization purposes and improved control, LEU will assume full responsibility of the process from end-to-end. We are targeting an implementation by Q1 2026.

Recommendation 4: Ensure that the responsible group develops and implements a process to

a. collect and deactivate third-party access cards from offboarded Board personnel.

Management Response: We concur with the finding and recommendation. As part of LEU's assumption of responsibility for the function, we will take over and update FS's current third-party access card process that includes collecting and deactivating cards for offboarded Board personnel. Additionally, we will integrate this process into LEU's overall lifecycle management of access cards. We are targeting an implementation by Q1 2026.

b. periodically reconcile third-party access card rights against human resources' list of active Board employees and contractors.

Management Response: We concur with the finding and recommendation. We will establish a periodic schedule wherein a list of active third-party access card holders will be compared with a list of active Board employees and contractors. We are targeting an implementation by Q1 2026.

Finding 3: The LEU Should Document the TSB's Responsibilities and Processes

Recommendation 5: Establish a policy that defines the TSB's responsibilities, and the standard operating procedures needed to fulfill those responsibilities.

Management Response: We concur with the finding and recommendation. We have drafted an initial TSB SOP which fully documents its responsibilities and processes. We are targeting an implementation by Q2 2026.

Finding 4: The LEU Should Further Establish Objectives for the TSB and Monitor Its Performance

Recommendation 6: Develop and document

a. measurable performance objectives for the TSB's responsibilities.

Management Response: We concur with the finding and recommendation. The TSB will develop performance objectives and measures and gather data to document its performance against the criteria at both the program and employee levels. These objectives and measures will be included in TSB's 2025-26 Align and Connect session and will be incorporated into applicable employees' 3C's start up agreements for the 2025-26 performance year. We are targeting an implementation by Q4 2025.

b. a monitoring process to assess the TSB's progress toward achieving those objectives.

Management Response: We concur with the finding and recommendation. We will develop a program level monitoring process to annually assess performance. At the employee level, monitoring will be done during individual 1:1 discussions, mid-cycle dialogues, and learning review wrap-up sessions. We are targeting an implementation by Q4 2026.

Abbreviations

DHS	U.S. Department of Homeland Security
FSL	facility security level
GAO	U.S. Government Accountability Office
ISC	Interagency Security Committee
LEU	Law Enforcement Unit
PIV	personal identity verification
SOP	standard operating procedures
TSB	Technical Security Bureau

Contact Information

General

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

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, or phone.

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

Phone: 800-827-3340