OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

MEMORANDUM

DATE: September 24, 2026

TO: Distribution List

FROM: Michael VanHuysen
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Management Alert 2026-MO-B-014R: *Findings from the Audit of the Board's Offboarding Process*

We initiated an audit in March 2025 to assess the Board of Governors of the Federal Reserve System's process for offboarding employees. Given the decentralized nature of certain parts of the offboarding process and the number of divisions with separate and varied activities in offboarding employees, we narrowed our audit scope to records management, security debriefings, and personal identity verification (PIV) card return and deactivation for all employees, including interns, who departed from the Board in 2024.

During our assessment of records management practices for departing employees, we identified and tested 26 instances of information removal requests and notifications involving departing employees. That testing identified gaps across multiple divisions in identifying and responding effectively to the removal of information by departing employees. This report focuses on one of the instances we tested because it best demonstrates the concerns we identified: (1) the inconsistent information security controls across multiple Board divisions; (2) the inconsistent and inadequate protocols for responding to information removal incidents by departing employees; and (3) more broadly, the Board's governance of its information security program.

The specific incident that this report focuses on concerns the Board's identification and response to the potential removal of Federal Open Market Committee (FOMC) classified and other sensitive Board information by a departing Division of International Finance (IF) employee. During our assessment of this removal incident, we became aware that the same IF employee had a prior information security incident during their IF employment involving FOMC classified information and additional instances involving data loss prevention (DLP) alerts related to the potential removal of sensitive information that IF stated were false positives. That prior history heightened our concerns about the apparent lack of diligence across multiple divisions in pursuing and resolving the removal incident that preceded the employee's departure from the Board.

Because of the potential severity of this possible information security incident, we referred the matter to our Office of Investigations (OI) in September 2025. OI reviewed this matter for potential misconduct and determined that there was not a sufficient basis to pursue this incident as a misconduct investigation, in part because available records did not provide a clear indication of what information the employee had removed before their departure and because OI confirmed that many of the DLP alerts related to the potential removal of sensitive information were, in fact, false positives. Although the available evidence did not support a misconduct investigation, the specific details regarding this incident help to illustrate the systemic concerns about the offboarding process we identified in this review.

We are issuing this management alert memorandum before completing our audit to detail our concerns. This potential incident highlighted information security risks and control breakdowns and deficiencies that we believe require the Board's immediate attention so that it can take appropriate corrective actions. In this memorandum, we describe the potential information security incident and findings that we discussed with you and your staff, as well as recommended improvements to strengthen controls to prevent, detect, and resolve potential information security incidents involving the unauthorized removal of sensitive Board information by Board employees, including departing employees. Given the sensitivity of the information in our review, portions of the public version of this report have been redacted. After issuing this management alert memorandum, we will resume our fieldwork activities related to our overall assessment of the adequacy of offboarding controls for records management, security briefings, and PIV card return and deactivation. The final report will also incorporate any implemented actions to address recommendations for these management alert findings.

Background

The Board's Records Management Program

The Board's Office of the Secretary, which includes the Records Management Program (RMP), administers and implements the *Removal or Disposal of Board Information by Departing Personnel* policy (*Information Removal Policy*) and the *Procedure for Removal of Information When Departing from the Board* (*Information Removal Procedure*). The *Information Removal Procedure* states that divisions review and approve the removal of public Board information, nonpublic Board information, personal papers, and research material. Departing employees must submit a request to remove any of the above information to their supervisor for review and approval. The RMP then confirms that supervisory review and approval have occurred before reviewing and approving that request.

The Board's Information Classification and Handling

The Board's *Information Classification and Handling Standard* describes seven levels of sensitivity (information classifications).[1] Employees must adhere to the designated controls and practices for handling and using information according to the information's format and classification. Information classifications commonly referenced in the policy,[2] from most to least sensitive, include the following:

- **Restricted-Controlled FR:** Applies to sensitive Board information that is highly to moderately confidential and that, if disclosed to or modified by unauthorized individuals, might cause serious loss, or have a serious negative effect on the Board's ability to perform its mission. Information owners use this designation rather than Restricted FR when dissemination of the information must be limited to a specific group of individuals.

- **Restricted FR:** Applies to sensitive Board information that is moderately confidential and that, if disclosed to or modified by unauthorized individuals, might cause significant loss, or have a significant negative effect on the Board's ability to perform its mission.

- **Internal FR/Official Use:** Applies to nonsensitive Board information with low confidentiality that is not officially declassified; does not meet the risk criteria for higher information classifications; and that, if disclosed to or modified by unauthorized individuals, might cause some loss or embarrassment to the Board.

The *Information Classification and Handling Standard* describes handling requirements for accessing, labeling, storing, and transporting each information classification type in both digital and printed formats. Specifically, this standard describes requirements for sending sensitive information through email and the appropriate use of encrypted storage devices. The standard states that nonpublic information, which is any information not rated as Public/Official Release or Nonconfidential, may not be disclosed outside the Board in any form without authorization. Emails containing sensitive Board information—which is any information assigned a Restricted-Controlled FR or Restricted FR classification—must be encrypted when

[1] The standard does not apply to information that is classified for national security purposes as defined in Executive Order 12958, as amended. Information referenced in this report is categorized using the Board's internal classification system and is unclassified for national security purposes.

[2] All seven Board information classifications, from most sensitive to least sensitive, are (1) Restricted-Controlled FR, (2) Restricted FR, (3) Sensitive Personally Identifiable Information, (4) Internal FR/Official Use, (5) Public/Official Release, (6) Nonconfidential, and (7) Personal/Nonwork.

sent to recipients outside the Federal Reserve System, and all emails, including personal emails, must be assigned the appropriate classification label. Additionally, all Board information must be stored on a trusted mobile storage device, and sensitive Board and FOMC classified information must only be stored on an encrypted trusted mobile storage device.

The Board also maintains the *Board Information Security Program*, which identifies which divisions to notify when information security incidents occur. The Division of IT also maintains the *IT Incident Response Manual*, which includes incident detection and response procedures for the Board's Information Security Operations (IS Operations) team.

FOMC Information Classification and Access

The FOMC's *Program for Security of FOMC Information* (*FOMC Program*) includes security procedures that govern the management of confidential FOMC information and are separate from the *Board Information Security Program*.[3] FOMC information is privileged information possessed by the seven-member Board of Governors, Federal Reserve Bank presidents, or System staff while performing their duties for, or pursuant to the direction of, the FOMC. The *FOMC Program* establishes the rules and describes the following three classifications for FOMC information:

1. **Class I FOMC:** Applies to sensitive information that must be handled at least as securely as Restricted-Controlled FR information

2. **Class II FOMC:** Applies to sensitive information that must be handled at least as securely as Restricted FR information

3. **Class III FOMC:** Applies to information that must be handled at least as securely as Internal FR/Official Use information

We refer collectively to information with any of these three classifications as *FOMC classified information*. The *FOMC Program* states that each level of FOMC classified information must be treated at least as securely as information in the corresponding Board information classification. Access to FOMC classified information requires that employees agree to the rules for handling confidential FOMC classified information. To maintain access, individuals must agree to the handling rules annually, comply with ethics policies, and complete annual FOMC classified information security training. FOMC classified information access may be terminated at any time if employees fail to abide by the handling rules.

The FOMC Secretariat prepares and manages access to FOMC classified information for policymakers, relevant staff members, and the public, as appropriate. The *FOMC Program* requires that the FOMC secretary, who is part of the FOMC Secretariat, or the general counsel refer all material known or suspected incidents involving FOMC classified information to us for investigation.

The Board's Data Loss Prevention Program

IS Operations uses DLP software to identify potential information security incidents. When an employee attempts to transmit sensitive Board information to an uncontrolled destination from specific browsers

[3] The FOMC oversees the Board's open market operations, reviews economic and financial conditions, determines the appropriate stance of monetary policy, and assesses risks to its long-run goals of price stability and sustainable economic growth.

and applications,[4] a DLP alert warns the employee that they may be violating the Board's *Information Security* policy and provides the employee with an option to cancel that action or enter a justification for proceeding. Examples of information removal activities that may trigger a DLP alert include copying sensitive Board files to an unencrypted USB device, printing sensitive documents, copying sensitive Board information from certain notepad applications to others, or uploading files to internet sites.

The IS Operations team notifies the RMP when a departing employee[5] triggers a DLP alert so that RMP can assess whether the employee's supervisor approved the information removal activity. As stated in the RMP's *Departing Employee Review* standard operating procedure (SOP), the RMP reviews the employee's submitted files after the supervisor's review and requests that the employee confirm through email that they deleted all confidential files in instances of unapproved information removals.

Scope and Methodology

We reviewed the Board's offboarding process controls for records management—specifically, the process for removing information by departing employees—to determine whether those controls operate effectively and mitigate information security risks. Our scope included all employees, including interns, who departed from the Board from January 1, 2024, to December 31, 2024. During our scope, the RMP received 18 information removal requests by departing employees and recorded 5 cases in which the IS Operations team notified the RMP of a potential removal of information by a departing employee. We also identified 3 cases of IS Operations notification samples that the RMP did not record. We tested all 26 of those instances. This report focuses on one of the IS Operations notification samples because it involved a high volume of DLP alerts, including for the removal of potentially sensitive Board and FOMC classified information. See attachment 1, "Additional Information Removal Observations from Other Divisions," for additional details from our testing. After issuing this management alert report, we will resume our fieldwork activities related to our overall assessment of the adequacy of offboarding controls for records management. That audit work will result in a separate report.

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

[4] Uncontrolled destinations include external email addresses; personal webmail; internet sites, such as Dropbox; CDs/DVDs; USB storage devices; and Secure Digital memory cards.

[5] The IS Operations team told us that it receives notifications of employees' departure dates through the Board's human resources system.

Confirmed and Potential Incidents Involving the Removal of Sensitive Information

During our testing in July 2025, we learned of a possible information security incident involving the potential removal of FOMC classified and Restricted FR information by an IF employee who, in February 2024, had announced plans to retire and a desire to remove files before their departure. The incident began shortly before the employee traveled in June 2024 to a country designated by the Board as restricted and continued up to and after the employee's retirement in July 2024, as outlined in the timeline below.[6] IF was not aware that the employee's June 2024 travel was to a Board-restricted country.

We became increasingly concerned about this incident after becoming aware of a previous incident of this employee improperly removing sensitive FOMC classified information by transferring it to an unencrypted USB device. Further, the employee continued to trigger additional DLP alerts by using an unencrypted USB device to transfer potentially sensitive information, which the division stated were false positives.

2021 FOMC Classified Information Incident

In 2021, the IS Operations team notified IF that the employee copied sensitive FOMC classified files to an unencrypted USB device. The IS Operations team's in-depth review revealed that the employee had copied hundreds of FOMC classified files to an unencrypted USB device. IF leadership confirmed the incident and notified the FOMC Secretariat, which noted the incident in an annual information security report. Documentation showed that the employee claimed that they mistakenly thought they were using an encrypted USB device to back up files. IS Operations requested that IF leadership advise the employee to use an encrypted device to back up their work, as required. IF leadership informed us that the employee's supervisor verbally advised them of the expectation to use an encrypted device but did not maintain written documentation of this counseling.

2023 Potential Removal of FOMC Classified Information

In 2023, the employee attempted to send sensitive FOMC classified information to their personal email account, which IF told us that the employee claimed was inadvertent. The FOMC Secretariat confirmed with the Division of IT that the email in this attempt was blocked and would not have been received by the employee's personal account, because emails with FOMC classification labels are automatically prevented from being sent externally. The FOMC Secretariat did not note this situation as an incident in its annual information security report because the system control prevented FOMC classified information from being exposed.

[6] The Board categorizes countries as *low risk*, *country of concern*, *high risk*, or *restricted* based on security risks posed by a traveler taking a mobile device to the foreign country. Restricted countries pose the greatest risk to Board information. In this situation, the employee did not hold a security clearance and therefore was not required to report planned personal travel to a foreign country. We recently issued a recommendation to the Board to broaden the scope of its foreign travel reporting to require employees with access to certain sensitive information, including FOMC information or confidential supervisory information, to report their personal foreign travel. 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.

Later in 2023, the IS Operations team again notified the FOMC Secretariat, IF leadership, and IF's Integrated Technology Solutions (ITS)[7] section that the employee potentially copied sensitive FOMC classified information to an unencrypted USB device. This transfer involved 83 files, including 3 files identified by the DLP alerts as potential FOMC classified information. The FOMC Secretariat did not classify the information transfer to a USB device as an incident based on IF's explanation that the DLP alerts were false positives and the files were publicly available. IF ITS held a conversation with the employee and reviewed document titles provided by the IS Operations team but did not review the files to verify the false positive explanations.

IF leadership told us that they asked for assistance from IS Operations and RMP to reduce the number of DLP false positives triggered by previously classified documents. IF ITS stated that the RMP believed that it was not possible to reclassify documents that had previously been categorized as FOMC classified. The IS Operations team also indicated to IF leadership that the DLP tool cannot easily determine whether information previously classified as FOMC has been downgraded, which could result in a false positive DLP alert that requires follow-up. To reduce the number of false positives, IF leadership verbally advised the employee to notify a member of IF ITS and IF leadership before future information transfers and the reasons for those transfers and to move information in bulk on a single day, if possible. This counseling did not reiterate or put into writing the prior verbal counseling about using an encrypted USB device when transferring sensitive information, including FOMC classified information. Despite the counseling in 2023, the employee engaged in similar activity before retiring in 2024, including using an unencrypted device, but did not inform IF ITS and IF leadership until after triggering 192 DLP alerts.

2024 Offboarding Information Removal Incident

Before retiring in 2024, the employee triggered more than 270 DLP alerts, as outlined below in figure 1 and table 1, because of printing, copying data to a notepad application, sending potentially sensitive information in emails to multiple personal email addresses, and transferring potentially sensitive files to a Board-issued unencrypted USB device.[8] The employee removed this information without seeking their supervisor's or the RMP's review despite previously being informed of the offboarding information removal procedures, prior counseling about bulk information transfers, and prior verbal counseling about using unencrypted storage devices.

Upon discovering the 2024 DLP events, we engaged in a series of follow-up conversations with IF, the FOMC Secretariat, the RMP, and IS Operations to better understand what occurred and management's rationale for its approach to the situation. We also conducted a review of the file names that triggered the DLP alerts, which indicated the possible removal of multiple sensitive documents.[9] We focused on the file names because, at the time of our review, most of the removed records no longer existed or could not be located and we did not have access to the former employee's storage devices.

[7] IF ITS supports the use of information technology, provides technology capabilities and solutions, and contributes to IF's technology strategy to support its mission. This function includes management and support for office automation activities, data management and analysis, and application development.

[8] The IS Operations team could not confirm whether the employee used the same device for the incidents from 2021 to 2024, but the device was unencrypted in all incidents.

[9] The employee told the colleague that they were requesting the document to prepare notes for another colleague who would assume their responsibilities upon retirement.

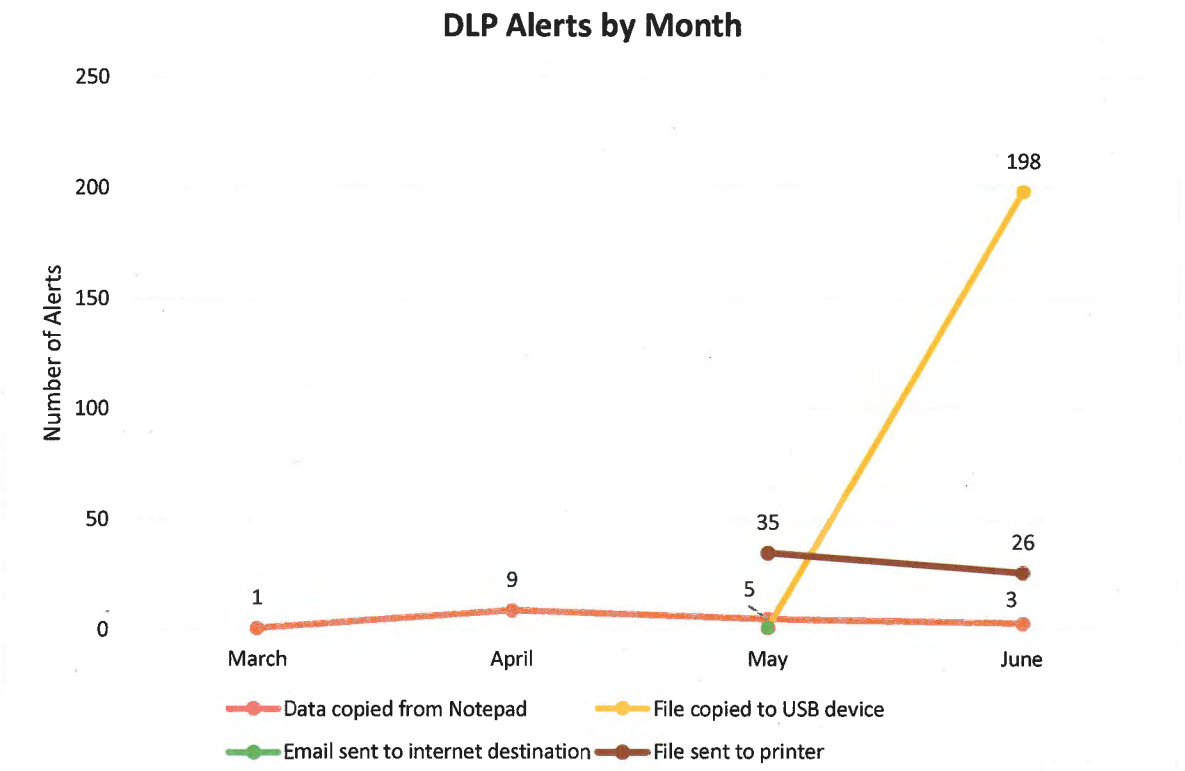
Because of the potential severity of this possible information security incident, we referred the matter to OI in September 2025. OI reviewed this matter for potential misconduct and determined that there was not a sufficient basis to pursue this incident as a misconduct investigation, in part because available records did not provide a clear indication of what information the employee had removed prior to their departure, and also because OI confirmed that many of the DLP alerts related to the potential removal of sensitive information were, in fact, false positives. Although the available evidence did not support a misconduct investigation, the specific details regarding this incident help to illustrate the systemic concerns about the offboarding process we have identified in this review. Several documents had file names that suggested they potentially contained forecast and economic data, including files that triggered 18 DLP alerts involving unknown data copied from notepad files. The DLP alerts that IS Operations sent to IF for review also included 16 files for which the file names only listed the file type, including four potential FOMC Class I files and one potential Restricted FR file, which the DLP tool indicated were printed email messages.

In total, in the 90 days before retiring in July 2024, the employee triggered 279 DLP alerts (figure 1 and table 1). The DLP tool identified 111 of these alerts as potentially involving sensitive FOMC classified information and 40 as potentially involving Restricted FR materials.[10] Further, 227 of the 279 alerts occurred in June 2024, with 192 occurring 3 days before the employee took what we understood to be a personal trip to a restricted country, which was followed by a separate personal monthlong international trip. IF personnel stated that they were unaware that the employee planned to travel to a restricted country.[11] See figure 2 for a timeline of this 2024 offboarding information security incident and the sidebar for risks of travel to restricted countries.

[10] IF leadership told us that the employee had a lengthy research career at the Board in which they analyzed formerly classified information.

[11] The employee did not have a security clearance at the time of the incident and therefore was not required to report their personal foreign travel to the Board. We have issued a report for the *Evaluation of the Board's Process to Monitor Foreign Travel* that includes a finding and recommendation related to the Board's foreign travel reporting requirements and broadening the personal foreign travel reporting requirements to apply to employees with access to sensitive information, such as FOMC classified information. 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.

Figure 1. DLP Alerts by Month, March–June 2024



Source: OIG analysis.

Note: In May and June, 24 alerts occurred on a weekend and over 80 occurred after 8:00 p.m. Of the 227 alerts in June, 93 percent occurred on or after June 16. The employee retired on July 2.

Table 1. Potential Classification of Information Identified by DLP Software, March–June 2024

Classification of Info	Total
External[a]	21
FOMC Class I	66
FOMC Class II	45
FR Classified[b]	7
Internal FR	47
Restricted FR	40
SPII/Board Personnel	35
No Classification Assigned	18
Grand Total	**279**

Source: OIG analysis.

[a] *External* is a term that the DLP software applies to indicate that information was moved outside the Board but is likely not Internal FR or above. This term is not an official internal Board classification level.

[b] *FR classified* is a blanket term that the DLP software applies to cover an overall event involving multiple files of varying levels of FR classification, including Internal FR and above. The DLP software may also apply this term to events that include information categorized as External. *FR classified* is not an official internal Board classification level and is not classified for national security purposes.

Figure 2. Information Security Incident Timeline, June 2024–July 2025

February 2024	**February 21:** IF ITS informed the employee about the Board's information removal process after the employee announced an intent to retire and the desire to remove files before separation. Despite the guidance that IF ITS provided to the employee about the removal process, the employee never formally requested to remove information.
June 2024	**June 10:** • IF ITS and the employee met to discuss the process for requesting to remove information. • The employee notified IF ITS that they would travel internationally on two different trips before separating. The employee stated that they would not take their Board laptop or PIV card on either international trip, that they were aware that they would not be able to use their Board laptop or PIV card after their last day of employment, and that they had coordinated with the Law Enforcement Unit for the return of the PIV card. • IF ITS approved the employee's request to retain their IT equipment past the retirement date. **June 20:** The employee notified IF leadership and IF ITS that they triggered DLP alerts while sending emails and transferring files to a Board USB device the previous day. The employee indicated that the alerts were false positives.[a] These files accounted for 192 of the 279 DLP alerts noted above, and 141 of the 192 files were identified by the DLP software as potentially sensitive FOMC classified information or Restricted FR. The employee traveled to the restricted country within the following 2 days. **June 21:** The IS Operations team notified the RMP, IF, and the FOMC Secretariat that the employee removed large volumes of information (see figure 1 for DLP alert history and table 1 for the DLP alert classifications). IF ITS emailed the employee to ask whether they had received approval to remove the files but did not immediately request that the employee return the USB or documents for review. **June 29–30 (on the weekend):** The employee returned to the United States from the restricted country. In response to messages from IF ITS about the initial 279 DLP alerts, the employee referred to their previous message sent 12 days before separation, which indicated that the alerts were false positives. • Over the weekend, the employee triggered 8 additional DLP alerts by printing at the office before traveling internationally again.
July 2024	**July 1:** The IS Operations team informed IF of the additional 8 DLP alerts and emails. IF ITS requested that the employee refrain from forwarding additional emails and informed them that IF needed to review the files on the USB device. **July 2:** The employee retired from Board employment. **July 8:** IF ITS contacted the former employee to arrange for a review and return all the removed files that had been copied to the USB device. The former employee responded and noted the monthlong international travel and stated an intent to provide the files upon returning to the United States.

August 2024	**August 1:** The former employee submitted files on an unencrypted USB device to IF ITS for review and returned their Board IT equipment. IF did not request the emails or printed documents, and the employee did not submit them for review.[b] We found that the files submitted by the employee on August 1 did not include any of the information that had triggered the DLP alerts. **August 22:** IF and RMP reviewed the information submitted by the employee but did not detect the significant discrepancy noted above. Nevertheless, the employee's supervisor and the RMP completed the review and only approved approximately 44 percent of the files for removal. IF's review involved running a script to identify files on the unencrypted USB device containing potentially sensitive Board information before conducting a manual review. The FOMC Secretariat did not participate in the review of the documents.
September 2024	IF ITS contacted the former employee twice regarding the return of the emails and printed documents. The former employee noted that they would respond but had tight deadlines on other matters. The employee did not respond again. IF did not attempt to contact the former employee after this final outreach. The IS Operations team, RMP, and the FOMC Secretariat also did not seek to determine the status of the incident once IF updates stopped.
July 2025	We began testing the 2024 information removal requests. The RMP contacted IF ITS to confirm the status of the incident. IF ITS informed the RMP that the former employee never responded and suggested that the RMP close the incident in its records removal tracker.[c]

Source: OIG analysis.

[a] Among other possibilities, false positives can occur when an email or document triggers a DLP alert for the apparent removal of sensitive information, despite the information not actually being sensitive.

[b] Submitting removed files for review is part of the standard process to review materials after the IS Operations team identifies that departing employees removed information. See *The Board's Data Loss Prevention Program* above.

[c] The RMP logs all requests for information removal in its departing reviews tracker.

Finding 1: The Board's Governance of Its Information Security Program and Enforcement of Its Controls Lacks Clarity

The 2024 information security incident that we detail above involved several Board divisions, including IF, which employed the individual and conducted the initial review and approval of submitted information; the FOMC Secretariat, whose information was at risk of compromise; the RMP, which had final review and approval of information removal requests; and IS Operations, which identified the unauthorized electronic removal of potentially sensitive information by this employee.

The Board has not established enterprise-level expectations to standardize escalation thresholds for information security events and specific coordination between affected divisions. However, the FOMC Secretariat, the RMP, and the IS Operations team maintain group-level procedures for incident escalation. Despite these group-level procedures, these three groups did not escalate the incident and instead relied

on IF to lead the resolution efforts. Specifically, the groups involved did not escalate the potential incident to the Core Response Group (CRG),[12] the Legal Division, or our office.

- IS Operations' *IT Incident Response Manual* states that IS Operations will engage the Legal Division and our office if there is confirmed or strong suspicion of data removal, or an uncooperative employee or manager or other concerning circumstances, and the *Incident Notification and Breach Response Plan* states that the information security officer (ISO)[13] will report known or suspected security incidents involving information rated Restricted FR to the CRG. During the 2024 incident, the IS Operations team and the ISO did not follow these response processes and only escalated the incident to IF leadership, the FOMC Secretariat, and the RMP.

- The RMP's *Departing Employee Review* SOP states that the RMP will notify the Legal Division of the removal of any Restricted FR material. The *FOMC Program* requires the FOMC secretary or the FOMC's general counsel to refer all material or suspected FOMC classified information incidents to our office for investigation. Nevertheless, we were informed that no escalation to the Legal Division or our office occurred.

- We identified the potential incident through our testing activities and alerted certain CRG members, including the Legal Division and our investigators, to the incident.

Additionally, no enterprisewide procedures exist to standardize how incidents are confirmed across the groups. In this instance, the groups involved did not appropriately assess and resolve the possible incident by reviewing the removed information effectively. As detailed in the timeline, IF and the RMP reviewed the information submitted by the employee but, during their review, failed to identify that the information submitted for review on the USB device did not include any of the information identified in the DLP alerts. The FOMC Secretariat also did not participate in the review of the documents that the employee submitted. None of the groups continued to follow up to obtain the relevant printed materials and emails.

The U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states that management should analyze and respond to information security risks so that they are effectively mitigated. Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity and serves as the first line of defense in safeguarding assets.

The Board has not defined clear roles, responsibilities, or coordination processes between divisions for handling potential information removal incidents, which contributed to the lack of clarity on each group's role in responding to the incident we reviewed. For example, the RMP told us that they believed that the IS Operations team was responsible for investigating incidents of unauthorized information removal, and IF personnel told us that they believed the IS Operations team handled escalations. IS Operations told us

[12] The CRG responds to security incidents by determining the harm posed by the incident and whether additional safeguards or corrective actions are appropriate. The CRG includes our office, the chief operating officer, the chief information officer, the senior agency official for privacy, the information security officer, general counsel, a congressional liaison officer, and a public affairs officer.

[13] The chief information officer has designated the ISO with the responsibility to execute all aspects of the day-to-day operation and maintenance of the Board's information security program and the program's compliance with the requirements of the Federal Information Security Modernization Act of 2014.

that it believed it could not do anything beyond alerting the RMP and the affected divisions, and FOMC Secretariat personnel told us that they believed that the Legal Division had been informed.

Additionally, based on our observation and follow-up, IS Operations, the RMP, and the FOMC Secretariat expected the employee's division to determine how to proceed. There are no enterprise-level procedures for confirming whether an incident occurred, establishing reasonable resolution time frames, or conveying coordination expectations in assessing a potential incident. For example, the RMP's information removal policy and information removal procedure do not include guidelines for what division supervisors should do when they receive notice from the RMP that an employee removed information without permission or how to respond to ongoing instances of information removal. Once the RMP notifies a division supervisor of a potential incident, the employee's division and its supervisor are responsible for contacting the employee, conducting a review, and informing the RMP of the results of the review.

The Board also has not defined clear thresholds for escalating apparent information removal incidents. The *Board Information Security Program* and *Incident Response Program* do not directly establish requirements for responding to or escalating instances of information removal. The *Incident Notification and Breach Response Plan* also does not include thresholds or criteria for reporting incidents to the CRG. In addition, as detailed in finding 3, the *FOMC Incident Response Program* does not include specific thresholds for escalation to the FOMC Incident Response Group (IRG), which is responsible for providing input to the FOMC secretary on whether an incident should be referred to our office.

Further, the Board has not established an enterprise approach for reviewing and escalating DLP alerts. In a 2024 audit, we recommended that the Division of IT document and implement a baseline review and escalation process for DLP alerts.[14] Resolving this open recommendation will help to standardize the DLP review process and ensure a similar scope of review for potential information removal incidents. The Division of IT is currently working with us to resolve this open recommendation; therefore, we will not include a recommendation for this issue in this report.

Each group's conflicting understanding of escalation and resolution responsibilities resulted in a general lack of clarity about how to proceed in addressing the incident and contributed to overreliance on the employee's division. This lack of clarity contributed to the incident remaining unresolved for over a year. Clear standardized processes and roles and responsibilities for all groups, as well as a sense of shared responsibility, will enable the Board to respond to such incidents appropriately.

Without implementing improvements to oversight, escalation, and incident response procedures, process weaknesses are likely to persist, undermining the effectiveness of the Board's overall information security program and increasing the risk of a major information security breach.

Recommendations

We recommend that the chief operating officer, in consultation with the Legal Division and the administrative governor,

1. Strengthen governance of the Board information security program by

[14] Office of Inspector General, *2024 Audit of the Board's Information Security Program*, OIG Report 2024-IT-B-020, October 31, 2024.

a. clearly describing ownership for assessing and resolving potential information security incidents and the roles and responsibilities of the IS Operations team, the RMP, division directors, the employee's supervisor, and information owners during apparent information security incidents involving unauthorized removal of Board information.

b. implementing escalation processes for information owners in affected divisions with requirements defining when to refer known or suspected instances of material unauthorized information removal to the affected division director, the director of the Division of IT, the general counsel, the CRG, and our office for investigation, and establishing how those escalations should occur.

2. Strengthen enforcement of the *Board Information Security Program* and *Information Classification and Handling Standard* to require

a. enhanced DLP monitoring of employees with a history of confirmed and other potential violations of these programs and standards.

b. appropriate remedial actions for employees with a prior history of information security violations including when dismissal may be appropriate.

Management Response

In response to our draft report, the Board concurred with our recommendations. For recommendation 1, the Board plans to implement processes and protocols to define roles and responsibilities and strengthen escalation alerts by the first quarter of 2027. For recommendation 2, the Board plans to create enhanced monitoring capabilities and escalation protocols through implementation of a new DLP solution by the third quarter of 2027.

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's Review During the Information Removal Incident Was Insufficient

IF's actions during the offboarding process and after the IF employee's retirement were not sufficient to safeguard Board information. Specifically, given the employee's prior FOMC classified information incident, history of generating DLP alerts that IF stated were false positives, failure to follow information removal procedures for departing employees, and information removal between known international trips[15] two days before retirement, IF's actions did not reflect appropriate diligence in reviewing the removed information to determine what occurred. For example,

- IF ITS granted the employee's request to retain Board IT equipment after their retirement date. IF ITS granted this request even though IF ITS was aware that the employee had been permitted by

[15] IF was aware of both of the employee's trips but informed us that they were unaware that one of the destinations was to a restricted country.

the Law Enforcement Unit (LEU) to keep their PIV card for that same period.[16] Although IF did not directly approve the employee retaining the PIV past the retirement date, the division was aware of the employee's PIV return request, past FOMC classified information incident, and history of generating DLP alerts when approving the equipment return accommodation request.

- After learning from the employee that they had triggered DLP alerts that they claimed were false positives, IF did not question the employee's claims or review the alerts and only asked the employee whether the information removal was approved after receiving an additional notification from IS Operations.

- Although IS Operations included all the DLP alerts and the associated file names in its notification to IF and indicated that IF should conduct the same review process used for all departing employees, IF did not confirm that all the potentially sensitive information had been returned. We determined that the information submitted by the employee for review did not include any of the information identified by the DLP alerts. As noted in finding 4, the *Information Removal Policy* does not provide guidance on the expected scope and depth of supervisor reviews, including in cases of unauthorized information removal.

- Despite the concerns that IS Operations expressed to IF regarding the unauthorized removal of information, IF stopped following up with this employee on the printed and emailed materials and did not escalate the incident to us. Specifically, IS Operations expressed concerns to IF ITS because of the employee's international travel, weekend printing, and previous history concerning information movement using the unencrypted device. These suspicious behaviors were indicative of possible insider threat risk activity (see sidebar).

GAO's *Standards for Internal Control in the Federal Government* states that management should enforce accountability of individuals performing their internal control responsibilities, which supports day-to-day attitudes and behaviors. The Board's Separating Employee Checklist states that employees must return PIV cards to the LEU before their departure date.

[16] The Separating Employee Checklist outlines all required tasks for departing employees, including the requirement to return PIV cards to the LEU before departing. However, the LEU was not informed of the employee's previous FOMC classified information removal incident or history of generating DLP alerts before approving the delayed PIV card return.

IF leadership told us that it is standard practice for employees who interact with external researchers and organizations to frequently share large volumes of public information. An IF interviewee also informed us that IF's business activities involve frequent international travel as well as collaboration with international institutions. This collaboration involves information removal and sharing. As an example, transferring files is often required for presentations at conferences and seminars, and economists often need to transfer documents to make them available on a non-Board device.

To support keeping their IT equipment after the planned retirement date, the employee stated to IF ITS and IF leadership that they would be completing Board work on the weekend between international trips and would be traveling on their retirement date. IF ITS accepted this explanation, knowing the employee had also been approved by the LEU to keep their PIV card, but did not independently seek to confirm that a business justification existed to support the accommodation—the division had not questioned what the employee was working on before retirement.

IF ITS also told us that it allowed the employee to retain Board equipment after separation because many of the employee's previous removal instances were false positives and because the employee's logical access would be disabled after separation.[17] However, even without logical access, an employee can still log in to a laptop or desktop using their PIV card or active directory password and access sensitive information saved locally on the hard drives. In this situation, the LEU confirmed that the employee's PIV remained active for 6 days after separation; however, IS Operations could not determine whether the employee used their PIV during that time.

Insider Threat Risk Indicators

The Board's *Insider Threat and Operations Security Awareness* training states that early identification and reporting of risk indicators allow for an appropriate response to mitigate risk. According to the training, threats include activities that jeopardize sensitive or proprietary information, and a potential risk indicator to be aware of is a pattern of security violations. Insider threat risk indicators are also outlined in the training, which describes the importance of detecting potential insider threats and reporting behaviors of concern to insider threat personnel or other designated officials.

The *Insider Threat and Operations Security Awareness* training is only required for Board employees holding national security clearances; therefore, IF may not have been aware of which suspicious behaviors were insider threat indicators to consider when responding to information removal incidents.

In March 2025, IF leadership requested insider threat training from the Division of IT and Intelligence, Insider Risk, and National Security Programs. Intelligence, Insider Risk, and National Security Programs provided an insider threat information session in April 2026.

[17] *Logical access* refers to access to Board applications and systems. We confirmed that the employee's logical access was disabled 1 day after their separation date.

Our *2024 Audit of the Board's Information Security Program* found that the Board has not defined a review and escalation process to ensure that DLP alerts are reviewed timely and that Board divisions determine their own review procedures.[18] Our recommendation for the chief information officer to implement a baseline review and escalation process for DLP alerts remains open; therefore, we limit the focus of our recommendations in this report and do not repeat this previously issued and open recommendation.

Additionally, as noted in finding 1, the Board has not defined clear roles, responsibilities, or coordination processes between divisions or clear thresholds for escalating apparent information removal incidents.[19] Because of this lack of guidance, IF did not have an available reference to follow during this incident.[20] However, even without this guidance, we believe IF could have taken reasonable measures to help resolve the incident (see sidebar). In our view, IF should calibrate its approach in determining whether information security incidents have occurred according to the division's heightened risk profile, which should result in enhanced division focus on adhering to the Board's information security requirements.

Potential Resolution Actions

We believe that IF—even with limited awareness of insider threat risk indicators—could have taken additional actions to respond appropriately to the suspicious behaviors and lessen the severity of the incident.

- Refer the employee for potential misconduct for continuing to violate rules on using personal email and unencrypted devices.
- Immediately request that the employee return the unencrypted USB device, printed documents, and emailed files for review after the first set of DLP alerts.
- Escalate the incident to our office before the employee's departure date.
- Review the DLP file names and compare them to information submitted for review on the USB to determine whether the files matched and whether an information security incident had occurred.

Management Actions

In July 2026, IF leadership told us about actions that the division has taken to reinforce leadership's commitment to following the Board's information security policies and procedures. Specifically, in October 2025, IF leadership updated the division's communication for departing employees to emphasize information removal requirements for departing employees. Additionally, IF leadership has communicated information security procedures to staff and supervisors in division-level meetings and emails, including the importance of DLP warning messages and the file review process for departing employees. Further, IF leadership has developed a draft information security incident reporting procedure that clarifies responsibility for tracking incidents and for notifying various IF division stakeholders, including the division director.

[18] Office of Inspector General, *2024 Audit of the Board's Information Security Program*, OIG Report 2024-IT-B-020, October 31, 2024.

[19] The Board operates separate programs that focus on information security incidents; however, these programs operate mostly independently, share little information, and do not clarify leadership responsibilities. See Office of Inspector General, *The Board Needs a More Robust Insider Risk Management Program*, OIG Report 2026-MO-B-010R, July 15, 2026.

[20] See finding 1 for specific recommendations to address these issues.

Recommendation

We recommend that the director of IF

3. Reinforce division leadership's commitment to following the Board's information security policies and procedures and expectations to avoid any similar future incidents by

    a. reviewing and identifying division improvement opportunities in the 2024 incident described in this report and discussing those lessons learned in a division-level forum that, at a minimum, includes all IF supervisors.

    b. developing and implementing an improvement plan that prioritizes a more active and diligent approach to responding to potential information security incidents.

Management Response

In response to our draft report, the Board concurred with our recommendation and stated it believes that IF's actions have addressed the recommendation.

OIG Comment

The completed actions described in the Management Actions section appear responsive to our recommendation. We will follow up to ensure that the recommendation is fully addressed.

Finding 3: The Board Did Not Escalate This Possible Incident Consistent with Expectations

The *FOMC Program* states that FOMC Class I, II, and III information must not be disclosed outside the Board without authorization, and the Board's *Information Classification and Handling Standard* states that sensitive Board and FOMC classified information can only be stored on an encrypted trusted mobile storage device. The *FOMC Program* requires the FOMC secretary or the FOMC's general counsel to refer all material or suspected FOMC classified information incidents to our office for investigation. The FOMC Secretariat's *FOMC Incident Response Program* describes the FOMC Secretariat's process to notify Secretariat leadership of potential security incidents and convene the IRG, which helps to determine next steps.

In 2021, IF notified the FOMC Secretariat that the former IF employee had copied FOMC Class I files to an unencrypted USB device. The FOMC Secretariat noted the incident in an annual information security report but did not immediately refer the matter to us.

Then, in 2023, the FOMC Secretariat learned that the employee had unsuccessfully attempted to send sensitive FOMC classified information to their personal email account. Later in 2023, the IS Operations team notified the FOMC Secretariat once more of the employee copying potential sensitive FOMC classified information to an unencrypted USB device. According to documents we reviewed, the FOMC Secretariat did not classify this information transfer to an unencrypted USB device as an incident because the employee claimed that the documents that generated the DLP alerts were all publicly available. The FOMC Secretariat relied on the employee's explanation to IF without verifying it, despite the employee's prior history of a confirmed information security incident and violation involving FOMC classified information.

FOMC Secretariat personnel told us that after learning of the DLP alerts in June 2024, [redacted] in the DLP alerts to determine that there was no credible evidence that the employee removed sensitive FOMC classified information. Further, after the employee provided IF with an unencrypted USB device for review following their retirement, the FOMC Secretariat did not participate in IF's and the RMP's review of the removed files to determine whether they contained sensitive FOMC classified information. The FOMC Secretariat also did not refer this incident to our office or the IRG.

The incident escalation criteria in the *FOMC Incident Response Program* do not include specific thresholds for information removal incidents, such as the volume or nature of the information removal, or instructions for how to address potential incidents involving employees with previous information security violations. Given the employee's history of generating DLP alerts related to the potential removal of sensitive information and previous confirmed FOMC classified information incident, we believe the apparent incident in 2024 should have been referred to us and the IRG as a suspected incident given the volume and information classification levels of the DLP alerts, proximity to the employee's retirement date, and the insider threat risk indicators noted in finding 2.

The *FOMC Incident Response Program* also does not specify when the FOMC Secretariat should take decisive action to identify incidents by conducting independent reviews of removed information or when to help contain incidents by potentially imposing temporary restrictions on FOMC access. FOMC Secretariat personnel told us that, as a matter of procedure, the FOMC Secretariat relies on division review of documents during potential incidents. In addition, an FOMC Secretariat official told us that it was told the incident had been escalated to the Legal Division and was being handled appropriately. However, an official in the Legal Division informed us that this escalation had not occurred.

By not pursuing potential measures to mitigate the risks of an ongoing incident, such as escalating the incident to our office and the IRG, the FOMC Secretariat's inaction contributed to the failure to recover the removed information. In addition, failing to define clear thresholds for escalation or circumstances when decisive action should be taken, such as temporary restriction of FOMC access and the independent review of removed materials, increases the risk that sensitive Board information is distributed without authorization and that employees involved in possible incidents that have not been addressed and resolved continue to remove more sensitive information.

Divisions such as IF are not directly responsible for controlling access to FOMC classified information. Therefore, in situations in which the responsible division does not show appropriate urgency in determining whether an information security incident occurred, the FOMC Secretariat should independently review the removed information. Additionally, it is important to review the contents of documents rather than relying solely on [redacted] The FOMC Secretariat should strengthen controls to safeguard FOMC classified information and respond more proactively to threats.

Recommendation

We recommend that the director of the Division of Monetary Affairs

4. Strengthen procedures related to the protection of FOMC classified information by
    a. defining the circumstances in which the FOMC Secretariat will be required to independently review the content of potential FOMC classified information removal.

b. establishing clear criteria and thresholds for when to escalate confirmed or suspected instances of FOMC classified information removal to the IRG.

c. establishing clear criteria and procedures for when and how the FOMC Secretariat can temporarily restrict FOMC access during ongoing confirmed or suspected incidents, including relevant stakeholders to consult; defined triggers; approval requirements; and expected time frames to review, approve, and restrict access.

Management Response

In response to our draft report, the Division of Monetary Affairs concurred with our recommendation. The Division of Monetary Affairs plans to recommend that the FOMC update the *FOMC Program*. The FOMC Secretariat plans to update its internal operational procedures to align with changes to the *FOMC Program* and with procedures and policies that the Board develops in response to recommendations 1, 4, and 5. The FOMC Secretariat plans to complete these updates by the fourth quarter of 2027.

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.

Finding 4: The Board's Response Protocols for Information Removal Incidents Are Unclear and Insufficient

The Board's policies and controls concerning the resolution of potential information removal incidents are unclear and insufficient to ensure consistent incident handling and resolution. Specifically, the *Information Removal Policy* and *Information Removal Procedure* lack guidance on the expected depth of information removal reviews, and the *Incident Response Program* does not specify that IS Operations may remove network connectivity from devices during instances of information removal threats, even when a pattern of prior incidents has appeared to develop. These policy gaps limit the tools available for the Board's response to potential information security incidents.

The RMP's Review of Unauthorized Removals by Offboarding Employees Are Insufficient to Ensure Adequate Control of Sensitive Information

During the 2024 information removal incident involving the former employee, the RMP relied on IF and the IS Operations team to confirm that all the removed information had been recovered. The RMP also did not identify that the employee did not return all the files identified in the DLP alerts. Additionally, the Legal Division was not notified that a potential removal incident had occurred involving Restricted FR material, as required by the RMP's internal SOP. We identified other situations that appear to indicate a pattern of the RMP accepting insufficient supervisor review of information removal requests by departing

employees throughout the Board. See attachment 1, "Additional Information Removal Observations from Other Divisions," for more details from our testing.[21]

The *Information Removal Procedure* states that an employee's supervisor and the RMP conduct independent reviews of information requested for removal. Additionally, in circumstances of unapproved removal by a departing employee, the RMP's *Departing Employee Review* SOP states that the RMP may conduct a formal review of removed information, after a review by a supervisor in the employee's division, and will notify the Legal Division of the removal of any Restricted FR material.

RMP personnel told us that divisions conduct their own reviews of information removal and the RMP does not enforce how division supervisors conduct these reviews. The *Information Removal Policy* also does not provide guidance on the expected scope and depth of supervisor reviews, including in cases of unauthorized information removal.

Allowing each division supervisor to determine the scope and approach of the review to be conducted increases the variability between the review scope, measures, and methods pursued. Further, relying on supervisor reviews, without confirming that all documents that need to be reviewed have been included in the scope of the review, undermines the effectiveness of any reviews that occur. Failing to adhere to established controls, such as escalating removal of Restricted FR material to the Legal Division, hinders the Board's ability to respond adequately to potential information security incidents.

The IS Operations Team Has Limited Authority to Prevent Ongoing Information Removal

The Board's *Incident Response Program* states that IT Security staff may remove network connectivity from compromised devices that may pose a threat to Board systems during cyber events. However, the *Incident Response Program* does not establish how to address employee violations of the *Information Classification and Handling Standard* or the circumstances in which enhanced DLP monitoring measures should be considered. The IS Operations team told us that its role in resolving potential information security events is limited to notifying the relevant division and not restricting employees' access to Board systems. Thus, in the incident involving the IF employee, despite the high volume of information removed, the employee's history of generating DLP alerts related to the potential removal of sensitive information, and other potential indicators of insider activity, the employee retained full access to Board systems and information before departure. In this situation, IS Operations told us that it did not escalate the incident to the CRG. We understand that IS Operations could not restrict an employee's access to Board systems without such an escalation to the CRG.

GAO's *Standards for Internal Control in the Federal Government* states that management should assign responsibility and delegate authority to key roles throughout the entity. Additionally, GAO states that controls related to the security of information systems include managing access to information systems.

Providing the IS Operations team, in consultation with ISO and the information owner's division director, authority to collaborate to restrict access to Board systems when circumstances warrant will help to minimize the risk of prolonged undetected and unresolved information security incidents. More effective

[21] After issuing this management alert report, we will resume our fieldwork activities related to our overall assessment of the adequacy of offboarding controls for records management. That work will result in a separate report and will not focus on the same issues addressed by recommendation 4.

escalations can help to further coordination and create a sense of urgency to assess whether an actual incident has occurred and to determine how best to proceed.

Recommendations

We recommend that the secretary of the Board

5. Update the *Removal or Disposal of Board Information by Departing Personnel* policy and the *Procedure for Removal of Information When Departing from the Board* to provide guidance on how in depth supervisory reviews should be, including in cases of apparent unauthorized information removal.

We recommend that the chief operating officer, in consultation with the Division of IT,

6. Authorize the ISO, in consultation with the information owner's division director, to restrict access to Board systems and define the limited circumstances when such a restriction may be warranted.

Management Response

In response to our draft report, the Board concurred with our recommendations. For recommendation 5, the Board has begun updating the *Information Removal Policy* and plans to update or create supplemental procedures and training materials by the second quarter of 2027. For recommendation 6, the Division of IT plans to add appropriate actions to processes and protocols related to its enhanced role in escalation, resolution, and data access restrictions by the third quarter of 2027.

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 5: The Board's Information Security Controls for Departing Employees Are Inconsistent

We identified deficiencies in the Board's controls to prevent unauthorized removal of sensitive Board information by departing employees and in its policies regarding the use of unencrypted removable media devices. The Board's offboarding policies and procedures for information removal lack guidelines for conducting consistent information removal lookback processes before an employee's departure date and the *Information and Classification Handling Standard* does not prohibit employees' use of unencrypted mobile storage devices.[22] The lack of standard lookback processes for departing employees and insufficient restrictions on the use of unencrypted devices by staff increases the risk of unauthorized removal of sensitive information before employees depart.

[22] Lookbacks involve reviewing an employee's DLP activity for a specified period.

The Board's Information Removal Lookback and Analysis Practices for Departing Employees Are Inconsistent

The Board's information removal review processes for departing employees are inconsistent, and not all divisions perform DLP lookbacks for departing employees. One Board division routinely performs an 18-month DLP lookback on employees upon notice of planned departures, which involves compiling and analyzing DLP alerts triggered during the 18 months before departure to identify potential inappropriate or suspicious actions. IF personnel told us that they perform weekly DLP alert reviews but do not document this process. In addition, we found instances involving other Board divisions that appeared to conduct lax reviews of information requested for removal by departing employees. For example, Board divisions often [redacted]

The National Insider Threat Task Force's leading practices guidance for departure procedures includes conducting a thorough review of departing employees' network activity within a defined time frame preceding the departure.

The Board does not have a standard procedure for independently verifying the contents of files in information removal activities and requests or for reviewing DLP logs before an employee's departure. [redacted] These inconsistent and ineffective verification practices hindered the Board's ability to respond timely and identify additional sensitive information among the removed files in the 2024 incident, resulting in potentially sensitive Board information remaining unaccounted for after the incident. These risks are particularly acute in specific divisions that routinely handle the Board's most sensitive information and regularly engage in foreign travel and collaborative activities that may heighten these risks. Such information can be easily retained or disseminated once removed.

The OIG's 2019 recommendation to the Division of IT concerning the Board's DLP review process about developing and implementing a Boardwide process to incorporate a review of DLP logs as part of employee and contractor offboarding processes to identify any potential unauthorized data exfiltration or access remains open. Prioritizing the resolution of this recommendation by developing a standardized DLP lookback review process for all departing employees will help to mitigate the risk of unauthorized information removal by separating employees.

The Board Did Not Adequately Restrict the Use of Unencrypted USB Devices on Board Equipment

The Cybersecurity and Infrastructure Security Agency, in its training on protecting data stored in devices, highlights how the use of encrypted removable storage devices (such as thumb drives, external hard drives, and Secure Digital cards) can prevent data from being accessed without authorization. The training further details how encryption is important for removable devices because they can often contain sensitive data and states that threat actors using malware or ransomware can install malicious code to access, read, edit, steal, or deny access to data stored on a device.

The Board's *Information Classification and Handling Standard* provides that agency information must only be stored on a trusted mobile storage device but does not require the mobile storage device be

encrypted unless the information is sensitive Board or FOMC classified information. The Board has only approved specific unencrypted USB devices, which the employee in the 2024 incident used.

The *Information Classification and Handling Standard* does not provide guidance on tracking the issuance of trusted unencrypted devices, revoking the ability to use trusted devices, or other measures to address violations of the standard. As of the time of our testing in 2025, no new unencrypted devices were permitted; however, employees can continue using previously allowed legacy unencrypted devices, as the employee in the 2024 incident did. Absent a change in Board policy, legacy devices could remain in use for years to store Board information despite the security risk they present. The IS Operations team told us that divisions acquire unencrypted mobile storage devices for the divisions' employees; therefore, it could not track which employees were permitted to use legacy unencrypted devices or whether employees were sharing devices. This lack of tracking prevented IS Operations from effectively determining whether these devices were used by employees without authorization or should be blocked.

In the 2024 incident described in this alert, IF allowed the retiring employee to continue using an unencrypted USB device to transfer Board information despite the employee's prior confirmed incident involving storing FOMC classified information on an unencrypted USB device, history of generating DLP alerts related to the potential removal of sensitive information, and IS Operations requesting that IF advise the employee to use an encrypted device after the 2021 incident and the verbal counseling on that topic afterward.

Given the employee's continued use of legacy unencrypted devices that appears to have remained unaddressed before 2024 and the potential severity of this 2024 information removal incident, insufficient restrictions on using unencrypted storage devices and failure to revoke authorization for violations increase the risk of unauthorized dissemination of sensitive Board information and increase the Board's vulnerability to malware and ransomware attacks using those storage devices.

Management Actions

In February 2026, the IS operations team told us that the Division of IT deployed system capabilities to block any encrypted or unencrypted USB device from connecting to Board equipment until the IT Security and Privacy group manually added it to an allowable device list. IS Operations provided preliminary documentation of these updates; we will follow up on the Division of IT's actions to ensure that recommendation 9 is fully addressed during our follow-up activities.

Recommendations

We recommend that the chief operating officer, in consultation with the Division of IT,

7. Prioritize resolution of the 2019 recommendation to develop and implement a Boardwide process for the review of DLP logs as part of offboarding processes and include a requirement to review all removed files identified in the lookback based on an analysis of potential severity and risks to the Board.

8. Develop a standard information transfer process to ensure that all departing individuals only remove information approved for release.

9. Develop and implement a process to eliminate the use of legacy unencrypted storage devices to conduct Board business and prohibit the use of new unencrypted storage devices.

Management Response

In response to our draft report, the Board concurred with our recommendations. For recommendations 7 and 8, the Board plans to implement a new DLP solution that will provide enhanced logging and monitoring to support offboarding processes by the third quarter of 2027. For recommendation 9, the Board plans to extend current capabilities to limit the use of all unencrypted storage devices and plans to implement a new DLP solution to provide enhanced monitoring of attempted data transfers by the third quarter of 2027.

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.

Conclusion

During our audit, we identified concerns with the response to an information security incident involving the potential removal of sensitive Board and FOMC classified information by a former IF employee. The 2024 incident was not fully resolved and the removed information was not fully retrieved. The failures in this situation were not limited to one division. The failures involved a collective lack of action across multiple divisions, and the limited follow-up activities that did occur were not commensurate with the accumulation of risks in this situation (even though, as noted, we determined there was not a sufficient basis to investigate the incident as a misconduct matter). IF did not conduct an effective review of the removed information, and the FOMC Secretariat took a hands-off approach to reviewing the DLP alert activity. The RMP and the IS Operations team also did not escalate the incident to those with the authority to resolve it.

The employee's ongoing pattern of potential and confirmed security violations; the employee's imminent departure; and the presence of multiple insider threat risk indicators, including multiple international trips, signaled the possibility that a credible insider threat incident and potential material information security breach had occurred. The lack of clarity in each division's role in responding to this incident highlights the need for a consolidated program to manage insider risks at the Board. Limited awareness of the employee's foreign travel plans demonstrates the importance of requiring travel reporting for employees with access to sensitive information, not just employees with security clearances. The OIG has also issued reports for the *Evaluation of the Board's Insider Risk Management Activities* and the *Evaluation of the Board's Process to Monitor Foreign Travel* that include additional findings and recommendations related to the Board's insider risk activities and foreign travel monitoring processes, respectively. In our estimation, this situation exemplifies risks and concerns highlighted in those other reports, including the need for a centralized and collaborative forum to monitor the resolution of potential insider risk incidents.

Our report contains recommendations designed to strengthen the Board's potential incident handling controls to avoid a recurrence and prevent information security incidents involving unauthorized removal of sensitive Board information by departing employees. After issuance of this management alert memorandum, we will transition to closing out fieldwork activities related to issuance of our final audit report, which will include findings and recommendations for the other in-scope areas. We will include in our final report any corrective actions your offices take in response to this memorandum.

We appreciate the cooperation we have received from the RMP, the IS Operations team, the FOMC Secretariat, and IF.

Attachments
cc: Mark E. Van Der Weide, General Counsel

Distribution:
Winona H. Varnon, Chief Operating Officer
Jeff Riedel, Chief Information Officer
Benjamin McDonough, Secretary of the Board
Beth Anne Wilson, Director, Division of International Finance
Trevor Reeve, Director, Division of Monetary Affairs

Attachment 1

Additional Information Removal Observations from Other Divisions

We tested all information removal requests made in 2024, including eight cases in which IS Operations notified the RMP of potential removal of sensitive information by departing employees. In addition to the incident detailed above, we identified the following instances that point to consistent gaps in the information removal review process for departing employees. After issuing this management alert report, we will resume our fieldwork activities related to our overall assessment of the adequacy of offboarding controls for records management.

- For three of the eight instances in which IS Operations notified the RMP of information removal, the removed information was not independently reviewed, including one instance in which the RMP and the employee's supervisor did not contact the employee at all and one in which they relied on screenshots of removed file names. These instances did not present the same risk characteristics as the 2024 incident and, therefore, did not warrant the same narrow focus.[23] Specifically, the information removed was classified significantly lower, and the DLP tool did not identify the possible removal of any potential Restricted FR or FOMC classified information.
- For three instances in which employees requested to remove information in accordance with the *Information Removal Procedure*, the supervisors' and the RMP's reviews were based on the employees' descriptions of documents or a list of the type of documents.
- Each division follows its own internal processes for supervisor review, and there is no standardized process that combines best practices from different divisions to mitigate the risk of unauthorized information removal.

We also noted the following examples of control deficiencies in the information removal review process. Although these instances are outside the scope of our project, we believe they demonstrate a need for increased governance of the information removal process noted in finding 1.

- The RMP did not become aware of improper information removal by a former employee in the Division of Research and Statistics until approximately a year after that employee's departure date.
- IF told us that a departed employee's information removal request was delayed because of technical issues and the manager's availability, and IF did not finish reviewing the request until over a year after the employee's departure date.

We will describe these observations in more detail in our final offboarding audit report.

[23] The IS Operations notifications in these instances included general information about external emails sent by the separating employee, whereas the 2024 incident notification included specific information about DLP activity involving the potential removal of sensitive information.

Attachment 2

Management Response

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

OFFICE OF THE
CHIEF OPERATING OFFICER

September 18, 2026

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

Dear Mr. VanHuysen:

Thank you for the opportunity to comment on the Office of the Inspector General's (OIG) draft Management Alert Report titled *Findings from the Audit of the Board's Offboarding Process*. We appreciate the OIG's work to develop the report and the recommendations.

We concur with the OIG's recommendations to strengthen the Board's governance of its information security program and enforcement of its controls. The Board takes these matters seriously and we plan to promptly take all required steps to implement all recommendations, and several are already underway. Additional monitoring capabilities that are already planned as part of a broader technology modernization initiative—and work underway to address previous OIG recommendations—should address many of these findings. The Division of Information Technology (IT) will play an enhanced role in the processes and protocols concerning review and monitoring, escalation, resolution, and access restrictions associated with data transmissions, and the Board will define and implement processes and protocols to address these matters—including updates to cross-divisional policies addressing critical handoffs between programs, and procedures related to staff training, review and escalation of data loss protection system alerts, and guidance to supervisors regarding departing employees.

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

Regards,

BENJAMIN MCDONOUGH Digitally signed by BENJAMIN MCDONOUGH Date: 2026.09.18 12:29:49 -04'00'

Benjamin McDonough
Secretary of the Board, Director of the Office of the Secretary

BETH WILSON Digitally signed by BETH WILSON Date: 2026.09.18 16:32:06 -04'00'

Beth Anne Wilson
Director of the Division of International Finance

JEFFREY RIEDEL Digitally signed by JEFFREY RIEDEL Date: 2026.09.18 11:57:30 -04'00'

Jeff Riedel
Director of the Division of Information Technology

TREVOR REEVE Digitally signed by TREVOR REEVE Date: 2026.09.18 11:52:00 -04'00'

Trevor Reeve
Director of the Division of Monetary Affairs

and

WINONA VARNON Digitally signed by WINONA VARNON Date: 2026.09.18 11:28:31 -04'00'

Winona H. Varnon
Chief Operating Officer

cc: Nelly Ramdass
Erin Cayce
Jim Dahl
Chip Young
Tannaz Haddadi
Kelly Gibbs
Leah Middleton

Response to recommendations presented in the Draft OIG Alert Report, *"Findings from the Audit of the Board's Offboarding Process"*

Finding 1: The Board's Governance of Its Information Security Program and Enforcement of Its Controls Lacks Clarity

Recommendation 1: Strengthen governance of the Board information security program by

a. clearly describing ownership for assessing and resolving potential information security incidents and the roles and responsibilities of the IS Operations team, the RMP, division directors, the employee's supervisor, and information owners during apparent information security incidents involving unauthorized removal of Board information.

b. implementing escalation processes for information owners in affected divisions with requirements defining when to refer known or suspected instances of material unauthorized information removal to the affected division director, the director of the division of IT, the general counsel, the CRG, and our office for investigation, and establishing how those escalations should occur.

Recommendation 2: Strengthen enforcement of the *Board Information Security Program* and *Information Classification and Handling Standard* to require

a. enhanced DLP monitoring of employees with a history of confirmed and other potential violations of these programs and standards.

b. appropriate remedial actions for employees with a prior history of information security violations including when dismissal may be appropriate.

Management Response:
We concur with the finding and recommendation 1. The Board will implement processes and protocols to address these matters, including defining roles and responsibilities and strengthening escalation alerts, as part of the broader technology modernization initiative. Remediation will concurrently address related recommendations associated with 2026-MO-B-010R. Target date: Q1 2027.

We concur with the finding and recommendation 2. The Board's will create enhanced monitoring capabilities and escalation protocols through implementation of a new DLP solution as part of the broader technology modernization initiative. Remediation will concurrently address related recommendations associated with OIG Report 2026-MO-B-010R. Target Date: Q3 2027.

Finding 2: The Board's Review During the Information Removal Incident Was Insufficient

Recommendation 3: Reinforce division leadership's commitment to following the Board's information security policies and procedures and expectations to avoid any similar future incidents by

a. reviewing and identifying division improvement opportunities in the 2024 incident described in this report and discussing those lessons learned in a division-level forum that, at a minimum, includes all IF supervisors.

b. developing and implementing an improvement plan that prioritizes a more active and diligent approach to responding to potential information security incidents.

Management Response:
We concur with the finding and recommendation. As described in the memo's management actions for this finding, the Division of International Finance has already taken actions that it believes addressed recommendation 3.

Finding 3: The Board Did Not Escalate This Possible Incident Consistent with Expectations

Recommendation 4: Strengthen procedures related to the protection of FOMC classified information by

a. defining the circumstances in which the FOMC Secretariat will be required to independently review the content of potential FOMC classified information removal.

b. establishing clear criteria and thresholds for when to escalate confirmed or suspected instances of FOMC classified information removal to the IRG.

c. establishing clear criteria and procedures for when and how the FOMC Secretariat can temporarily restrict FOMC access during ongoing confirmed or suspected incidents, including relevant stakeholders to consult; defined triggers; approval requirements; and expected time frames to review, approve, and restrict access.

Management Response:
The Division of Monetary Affairs concurs with the recommendation to strengthen procedures related to FOMC classified information and will recommend the FOMC incorporate updates to its Program for Security of FOMC information (Program). The FOMC Secretariat will update its internal operational procedures to align with any FOMC-approved changes to the Program, as well as with relevant procedures and policies relating to review triggers, escalation thresholds, and access restriction protocols the Board will develop in response to Recommendations 1, 4, and 5. Implementation of changes within the division's purview will occur throughout 2027, with completion by Q4, subject to the FOMC's approval of our recommendations.

Finding 4: The Board's Response Protocols for Information Removal Incidents are Unclear and Insufficient

Recommendation 5: Update the *Removal of Board Information by Departing Personnel* policy and the *Procedure for Removal of Information When Departing from the Board* to provide guidance on how in depth supervisory reviews should be, including in cases of apparent unauthorized information removal.

Management Response:
We concur with the finding and recommendation. Effort is already underway to update the Removal policy, with updates to or creation of supplemental procedures and training materials. Target Date: Q2 2027.

Recommendation 6: Authorize the ISO, in consultation with the information owner's division director, to restrict access to Board systems and define the limited circumstances when such a restriction may be warranted.

Management Response:
We concur with the finding and recommendation. With the Division of Information Technology's (IT) enhanced role concerning escalation, resolution, and access restrictions associated with data transmissions, the division will add appropriate actions to updated processes and protocols to address this finding. Target Date: Q3 2027.

Finding 5: The Board's Information Security Controls for Departing Employees Are Inconsistent

Recommendation 7: Prioritize resolution of the 2019 recommendation to develop and implement a Boardwide process for review of DLP logs as part of offboarding processes and include a requirement to review all removed files identified in the lookback based on an analysis of potential severity and risks to the Board.

Management Response:
We concur with the finding and recommendation. The Board will be implementing a new DLP solution as part of the broader technology modernization initiative that will provide enhanced logging to support offboarding processes. Remediation will concurrently address related recommendations associated with OIG Report 2019-IT-B-016. Target Date: Q3 2027.

Recommendation 8: Develop a standard information transfer process to ensure that all departing individuals only remove information approved for release.

Management Response:
We concur with the finding and recommendation. The Board will be implementing a new DLP solution as part of the broader technology modernization initiative to provide enhanced monitoring to ensure only authorized information is transferred to departing staff. Target Date: Q3 2027.

Recommendation 9: Develop and implement a process to eliminate the use of legacy unencrypted storage devices to conduct Board business and prohibit the use of new unencrypted storage devices.

Management Response:

6

We concur with the finding and recommendation. The Board will extend current capabilities to limit the use of unencrypted storage devices to include all devices previously approved through exception requests. In addition, the Board will be implementing a new DLP solution as part of the broader technology modernization initiative to provide enhanced monitoring of attempted data transfers. Target Date: Q3 2027.