Evaluation Report
2026-MO-B-009R
June 15, 2026

Board of Governors of the Federal Reserve System

The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks

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, 2026-MO-B-009R, June 15, 2026

The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks

Findings

The Board of Governors of the Federal Reserve System's international travel processes for its employees related to monitoring and mitigating their international travel risks should be strengthened. The Board does not have a formal program to prepare employees before international travel on how to identify and mitigate possible threats to personal safety and Board information. Employees also do not receive post-travel questionnaires to report suspicious activity that could help mitigate potential security risks for future travelers. Further, the Board does not have (1) a program to aggregate and analyze available employee travel data; (2) a process to share travel-related information among relevant groups to identify and escalate travel risks, when appropriate; or (3) a process to assess compliance with its international travel reporting requirements.

The Board limits its international travel reporting requirements to employees with a security clearance and does not require reporting by employees with access to sensitive Federal Reserve System information. Finally, the Board does not consistently inform division designated travel reviewers of travel risks before their review of employee requests to use Board devices while on international travel. Without these practices, the Board limits the support it offers to its divisions, which increases operational and information security risks.

Recommendations

Our report contains six recommendations designed to strengthen the Board's international travel processes to minimize the risks presented to Board information and Board employees while traveling abroad. In its response to our draft report, the Board concurs with our findings and recommendations and outlines planned actions to address the recommendations. We will follow up to ensure that the recommendations are fully addressed. Given the sensitivity of the information in our review, portions of the public version of this report have been redacted.

Purpose

We conducted this evaluation (1) to assess whether and ensure the Board's reporting and monitoring processes for international travel by employees follow standards and guidance for mitigating undue foreign influence and (2) to assess the Board's processes for monitoring international travel with Board devices to ensure protection of Board information. We assessed employee travel data from multiple sources from March 1, 2023, through March 31, 2025, as well as a sample of security alerts from February 1, 2025, through March 31, 2025.

Background

International travel helps facilitate the Board's collaboration efforts with other central banks and other foreign governmental and nongovernmental entities. International travel introduces information security and physical risks that are not present when traveling within the continental United States. It is common for foreign adversaries to target U.S. government employees to acquire nonpublic information.

To help address these risks, the Office of the Chief Operating Officer and the Division of Information Technology primarily manage the Board's international travel processes. Specifically, the Office of the Chief Operating Officer manages international travel reporting for clearance holders, and the Division of IT manages the international travel with Board devices processes for all travelers, including monitoring for any suspicious activity related to those devices.

Recommendations, 2026-MO-B-009R, June 15, 2026

The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks

Finding 1: The Board Should Better Inform Employees of International Travel Risks

Number	Recommendations	Responsible office
1	Leverage existing System resources to develop and implement a process to provide pretravel briefings covering threat and risk awareness to employees traveling on official business trips or taking Board devices to high-risk and restricted countries, at a minimum.	Office of the Chief Operating Officer and Division of Information Technology
2	Leverage existing System resources to develop and implement a process to provide Board-specific travel threat awareness trainings for employees in high international travel or senior positions and employees in high traveling divisions, at a minimum.	Office of the Chief Operating Officer and Division of Information Technology
3	Leverage existing System resources to develop an optional post-travel questionnaire and establish a process to provide the questionnaire to Board employees who are required to report international travel based on the implementation of recommendation 6, at a minimum.	Office of the Chief Operating Officer and Division of Information Technology

Finding 2: The Board Does Not Consolidate and Assess International Travel Data to Identify and Escalate International Travel Risks

Number	Recommendation	Responsible office
4	Establish a program that consolidates and assesses international travel data available to Board divisions regarding employee international travel, including a. creating capabilities to aggregate and analyze foreign travel data from available sources, including the travel reimbursement platform, the security clearance holder reporting application, and the travel device request platform. b. developing a process to reconcile clearance holder unreported travel data. c. expanding foreign travel data analysis beyond risks related to travel with devices and developing a process to conduct travel trend analysis including indicators of suspicious travel patterns, define levels of organizational risk tolerances for suspicious travel activity and follow-up processes to understand that activity and escalate any potential threats to the appropriate division and insider risk program, and identify potential travel-related threats that should be factored into training materials.	Office of the Chief Operating Officer and Division of Information Technology

Finding 3: The Board Does Not Require International Travel Reporting for Employees with Access to Sensitive Information

Number	Recommendation	Responsible office
5	Strengthen travel reporting requirements by a. determining which Board positions or division employees should be required to report personal international travel before departure based on access to System sensitive information. b. updating policies and procedures detailing travel reporting requirements for relevant positions and divisions with access to System sensitive information. c. designating a program to monitor reported travel and defining risk monitoring and threat awareness reporting expectations for that program.	Office of the Chief Operating Officer

Finding 4: The Board Does Not Have a Process to Inform All DDTRs of Travel Risks Before Reviewing Requests for International Travel with Board Devices

Number	Recommendation	Responsible office
6	Develop a process to ensure all DDTRs are informed of country-specific risks at least annually and provide training when updates occur to the international travel with mobile devices process.	Division of Information Technology and Office of the Chief Operating Officer

Contents

Introduction

Objective

Our objective was to assess whether and ensure the Board's reporting and monitoring processes for international travel by employees follow standards and guidance for mitigating undue foreign influence and to assess the Board's processes for monitoring international travel with Board devices to ensure protection of Board information. To accomplish our objective, we reviewed Board policies, standards, manuals, and guidance for employee international travel. We also interviewed Board personnel from divisions involved in administering these policies and standards, as well as from divisions with frequent travelers. Further, we analyzed Board international travel data for business and personal purposes from March 1, 2023, to March 31, 2025, and tested a sample of travel-related security alerts from February 1, 2025, through March 31, 2025. Details on our scope and methodology are provided in appendix A.

Background

The Board routinely collaborates with foreign central banks, international organizations, academic institutions, other financial regulators, and foreign governments. International travel helps support these collaborative activities. Travel to and through foreign countries and U.S. territories introduces information security risks to Board devices and physical risks to employees that are not present when traveling within the continental United States.

Risks Faced by the Board

Attempts by foreign adversaries to target U.S. government employees, including Board employees, are common. Further, the risk that Board employees may be targeted for espionage activities increases when they travel to certain foreign countries, especially those employees with highly valued expertise, experience, and access to information—specifically sensitive, nonpublic information—that these adversaries and competitors would find useful. Highly sophisticated and capable foreign intelligence services have targeted Federal Reserve System personnel. For example, China has targeted and obtained information from the System, as evidenced by an insider risk incident (see sidebar). Common foreign collection methods include targeting government personnel during international visits and at international conferences, as well as using academic solicitation to obtain sensitive or national security information.

THE BOARD FACES THREATS BY FOREIGN INTELLIGENCE ENTITIES

A former Board employee shared sensitive Board and Federal Open Market Committee information and other documents with Chinese government intelligence officers. These officers posed as students at an academic institution and communicated by email. The employee had multiple trips funded to China to share information on System forecasts and financial development plans.

According to several government sources, foreign intelligence agents are targeting the employees of financial institutions in both the public and private sectors,

including the Board. Most of the Board workforce can access sensitive System information, such as Federal Open Market Committee (FOMC) information and confidential supervisory information (CSI):[1]

- **FOMC information** includes all privileged information that comes into the possession of the Board members, Federal Reserve Bank presidents, or System staff in the performance of their duties for, or pursuant to the direction of, the FOMC. The FOMC is responsible for setting the monetary policy of the United States and, in connection with its meetings, FOMC members are provided with sensitive, nonpublic economic and financial information.
- **CSI** includes information that was created or obtained as a result of the Board's supervisory, investigatory, or enforcement activities, including activities conducted by a Reserve Bank under delegated authority. For example, pursuant to its regulatory supervision of financial institutions, the Board obtains information such as bank examination reports, supervisory ratings, and nonpublic information reported by financial institutions.

In addition to the types of sensitive information listed above, the loss of nonpublic information related to people, processes, technology, and facilities, such as internal business processes or proprietary research, can result in security risks to the Board. Further, information that may not seem particularly significant standing alone can sometimes be combined with other information previously collected by foreign adversaries to provide a more complete and comprehensive understanding regarding a sensitive matter affecting U.S. interests or institutions.

The Board's Process for Monitoring International Travel

Two divisions primarily manage the Board's international travel:

- **Office of the Chief Operating Officer's Intelligence, Insider Risk, and National Security Programs (IINS).** Board employees with national security clearances must report any international travel plans, both business and personal, to IINS before travel. The Office of the Director of National Intelligence (ODNI) requires such reporting for personal travel but allows agencies to determine the reporting requirements for official travel.[2]
- **Division of Information Technology.** The Division of IT's *International Travel with Mobile Devices Standard* outlines the processes travelers must follow before and during international travel. The process differs based on the trip's destinations and layovers as well as the highest associated country risk classification (figure 1). For each country, the Board designates a risk classification

[1] Board employees may access FOMC information and CSI if they (a) have a need to know, (b) are a U.S. citizen or declared the intent to become a permanent resident and U.S. citizen and were determined to be suitable based on background investigation results, (c) are deemed eligible based on Board policy, and (d) are designated by select Board officials. Access to FOMC information and CSI percentages are based on the total number of Board employees as of January 5, 2026; the number of employees eligible for FOMC information access as of January 2, 2026; and the number of employees eligible for CSI access as of January 3, 2026.

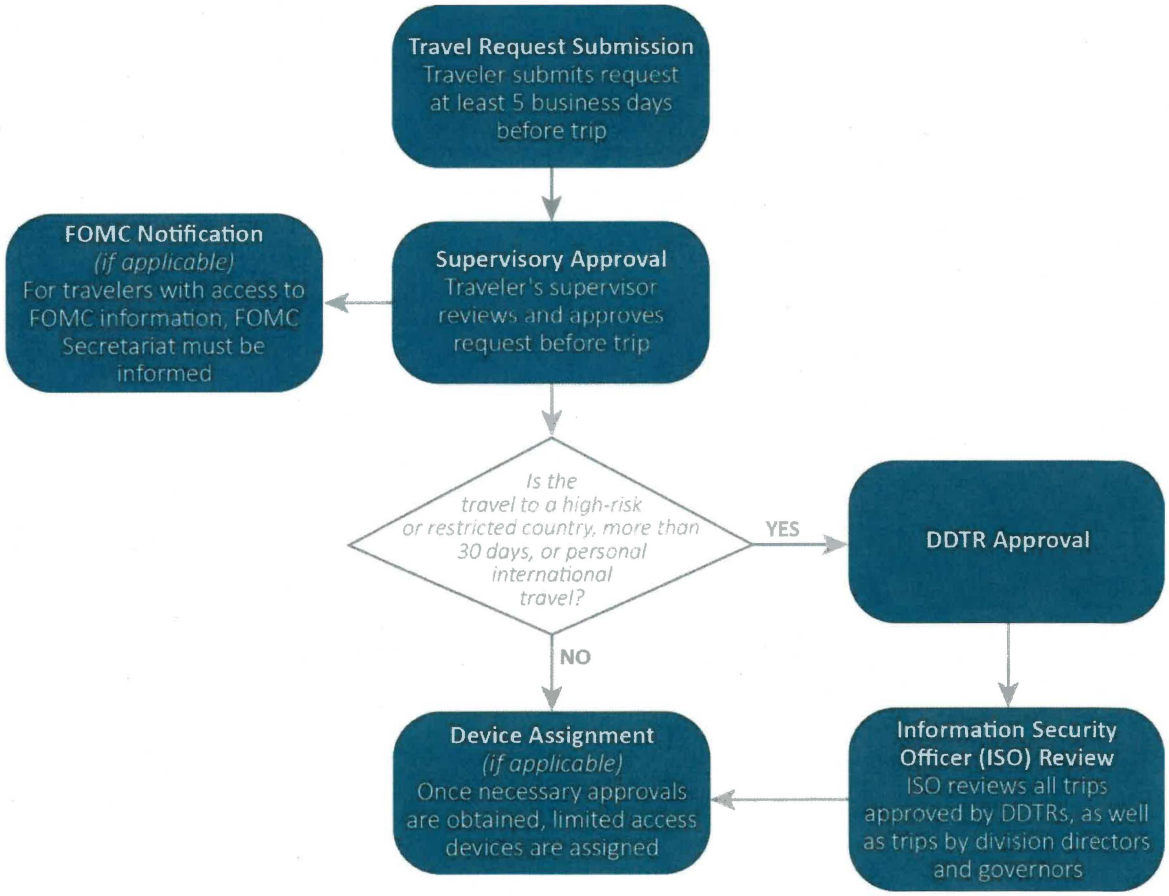
[2] Office of the Director of National Intelligence, Security Executive Agent Directive (SEAD) 3, effective June 2017, https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf. SEAD 3 details reporting requirements across the federal government for all individuals who have access to classified information or hold a sensitive position, including for foreign travel. SEAD 3 requires individuals who have access to classified information or hold a sensitive position to submit an itinerary for personal foreign travel and receive approval from the agency before the travel. The Board does not require such employees to receive approval before personal foreign travel. According to a Board official, the Board does not inform employees where they can and cannot travel.

based on the level of security risk and threat to Board information or operations when a traveler takes a Board device abroad. The country risk classifications are

- low risk: pose little to no threat
- countries of concern: pose a credible or potential threat
- high risk: pose a high potential threat
- restricted: pose a definite, serious threat to Board information or operations

The Division of IT updated the *International Travel with Mobile Devices Standard* in January 2025 to include a division designated travel reviewer (DDTR) role within each division, a high-risk country risk classification, and notifications to the FOMC Secretariat for international travelers with access to FOMC information. Further, the Board provided new *International Travel Risk Decision Guidance* for approvers to review travel requests based on the risks to Board information and systems. The guidance offers a decision matrix DDTRs can use when reviewing requests based on the employee's itinerary and requested device.

Figure 1. International Travel with Board Devices Process

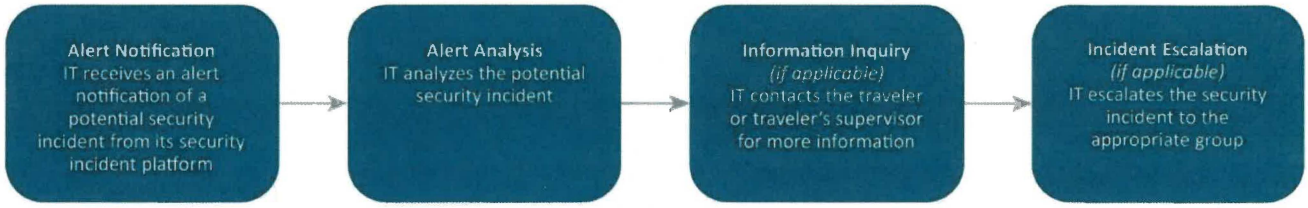


Source: OIG analysis of Board documents.

Incident Response Program Procedures

The Division of IT follows its *Incident Response Program* standard dated October 2017, to detect, respond, and report all cybersecurity incidents that may compromise the availability, integrity, and confidentiality of Board information. Specifically, the Division of IT monitors for any suspicious activity related to Board devices, including the unauthorized presence of Board devices in foreign countries, data loss protection events before travel, emails to or from restricted countries, and instances of employees visiting websites hosted by restricted countries regardless of the user's physical location (figure 2).

Figure 2. Division of IT's Security Alert Response Process



Source: OIG analysis of Board documents.

The Board's Training Related to International Travel

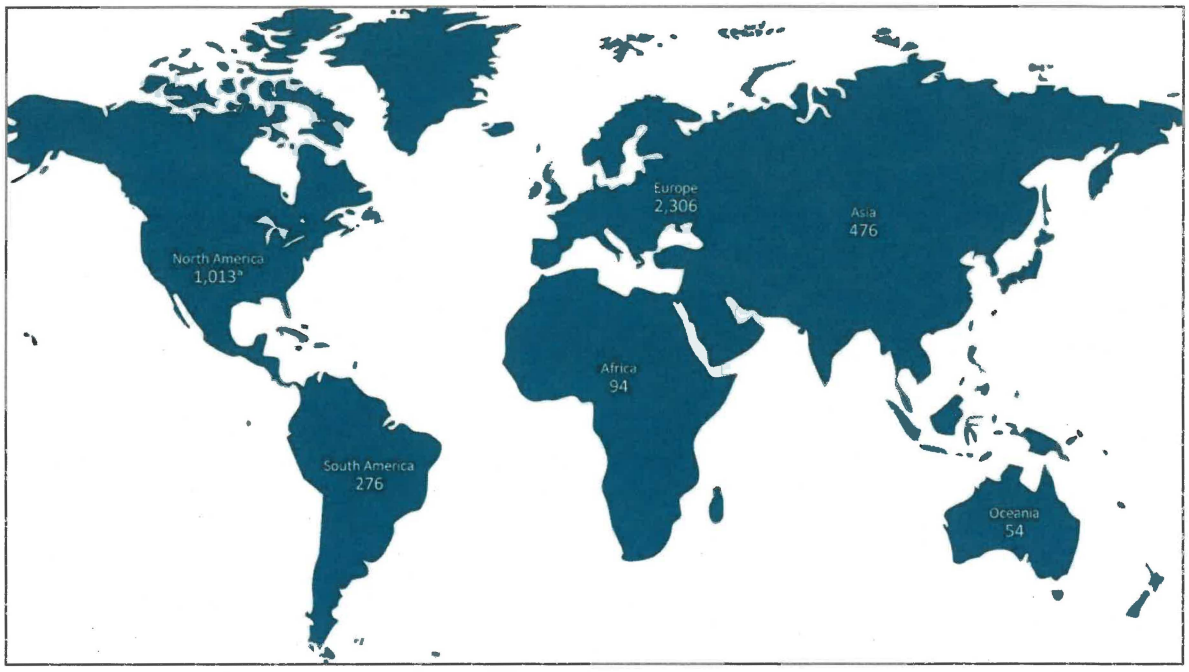
The Board provides employees two annual training courses that discuss international travel topics. An employee's access to information determines which trainings are required. Specifically, all Board employees must take the Division of IT's Security Awareness and Privacy Training, which outlines a wide range of Board security and privacy policies and procedures, including the *International Travel with Mobile Devices Standard.* Only Board employees with security clearances, which represents approximately 12 percent of the Board's workforce, must take IINS's Insider Threat Awareness and Safeguarding Classified National Security Information Training.[3] The training outlines Security Executive Agent Directive (SEAD) 3's international travel reporting requirements and potential insider risk indicators, such as unexplained international travel, foreign targeting and recruitment, and the risks of potential foreign influence.

The Board's International Travel Data

The Board maintains employee travel data from multiple sources, including requests to travel with Board devices and travel reported by clearance holders. We aggregated these data sources to identify the most frequently visited countries and the Board divisions with the most international travel. Figures 3, 4, and 5 outline the results of our analysis. See "Appendix A: Scope and Methodology" for detailed descriptions of the information contained in our data sources.

[3] The percentage of employees with a security clearance is based on security clearance case management system data as of January 2, 2026, and the total number of Board employees as of January 5, 2026, which excludes interns and contractors and includes OIG employees. Security clearances are governed by IINS.

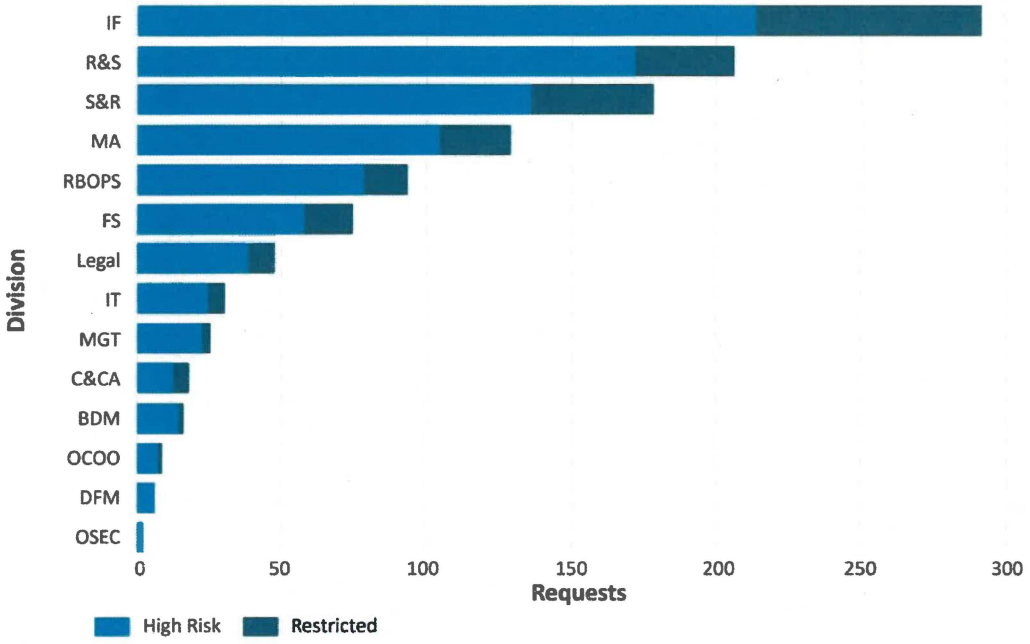
Figure 3. Number of Trips with Board Devices, by Continent (Including Layovers), March 2023–March 2025



Source: OIG analysis of the travel device request platform data.

[a] Excludes domestic travel within the United States.

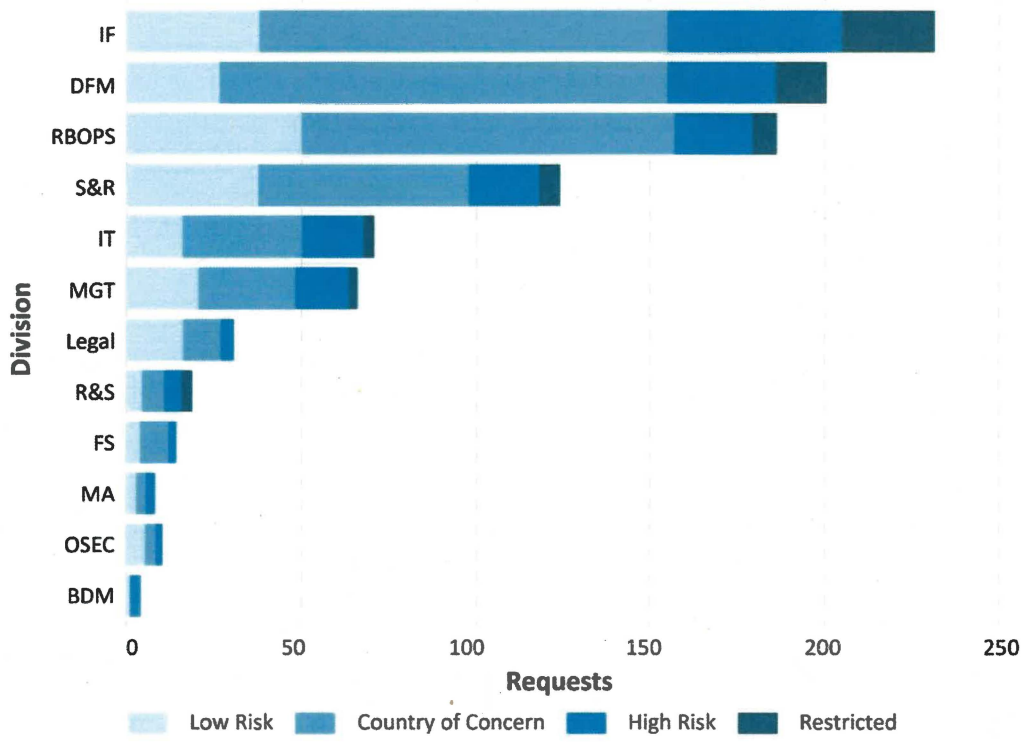
Figure 4. Travel with Board Devices to High-Risk and Restricted Countries, by Division, March 2023–March 2025



Source: OIG analysis of the travel device request platform.

Note: Travel with Board devices to high-risk and restricted countries includes business trips, personal trips, and trips for business and personal purposes. The Board divisions listed in this figure are International Finance (IF), Research and Statistics (R&S), Supervision and Regulation (S&R), Monetary Affairs (MA), Division of Reserve Bank Operations and Payment Systems (RBOPS), Financial Stability (FS), Legal Division, Division of IT, Management (MGT), Consumer and Community Affairs (C&CA), Division of Board Members (BDM), the Office of the Chief Operating Officer (OCOO), the Division of Financial Management (DFM), and the Office of the Secretary (OSEC).

Figure 5. Clearance Holder Travel, by Division, March 2023–March 2025



Source: OIG analysis of the clearance holder reporting platform.

Note: The Board divisions listed in this figure are International Finance (IF), Division of Financial Management (DFM), Division of Reserve Bank Operations and Payment Systems (RBOPS), Supervision and Regulation (S&R), Division of IT, Management (MGT), Legal Division, Research and Statistics (R&S), Financial Stability (FS), Monetary Affairs (MA), the Office of the Secretary (OSEC), and the Division of Board Members (BDM).

International Travel Leading Practices and Guidance

We identified the following leading practices for monitoring international travel through outreach with the Federal Reserve Bank of New York (FRB New York), the nationwide Federal Reserve Information Technology (National IT) organization that supports the 12 Reserve Banks, and a peer federal financial regulatory agency.[4] We compared these practices to the Board's foreign travel activities to identify potential improvement opportunities for the Board to implement.

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

Table 1. Leading Practices for Monitoring International Travel

	FRB New York	National IT	Peer Federal Financial Regulatory Agency
Pretravel briefings	Provided to employees on official business trips to countries classified as countries of concern or higher. Informed travelers of cyber risks, crime, safety, and host country threats to better position them to identify and mitigate threats to their personal safety and devices.	Collaborated with FRB New York to expand briefings to other Reserve Banks for employees on official business trips to countries classified as countries of concern or higher.	Provided to all employees and executives traveling internationally. Focused on country-specific threats, including crime, personal safety, and host country threats.
Threat awareness briefings and trainings	Conducted annual briefings for economists and researchers to share information on threats to intellectual property and System information, such as espionage threats and threats when traveling to international conferences.	Partnered with the National Institute of Standards and Technology to conduct security training for Reserve Bank researchers on international travel risks, malign foreign recruitment, and safeguarding information.	n.a.
Post-travel questionnaires	Provided an optional post-travel questionnaire that requests information about device usage and threats, information security, and unusual experiences during official business travel.	Collaborated with FRB New York to produce optional post-travel questionnaires for official business travel.	Provided optional post-travel forms for personnel with a security clearance.
Travel reporting for nonclearance holders	Required researchers to report all official business international travel.	n.a.	n.a.

Source: OIG analysis.

Note: FRB New York provided briefings and questionnaires as part of its Threat Awareness and Reporting Operation program to its employees, three other Reserve Banks (Atlanta, Philadelphia, and Richmond), and the Board's Division of Reserve Bank Operations and Payment Systems.

n.a. not applicable.

Additionally, we identified several frameworks and guides that provide federal agencies with strategies to safeguard information and employees during international travel. These practices aim to strengthen federal protective programs and reduce security risks. Appendix B outlines the source materials we used to identify leading practices.

Finding 1: The Board Should Better Inform Employees of International Travel Risks

The Board does not have a formal program to prepare employees before international travel on how to identify and mitigate possible threats to personal safety and Board information while abroad. Specifically, we found that Board employees do not regularly receive pretravel briefings on international travel risks, including foreign targeting and recruitment, country-specific threats, and mitigation strategies. According to Board officials, these briefings occur on an ad hoc basis, including for Board governors and other executive officials. In addition, the Board's training and resources for international travel are not specific to risks Board employees may encounter in high-risk or restricted countries.[5] While we found that IINS conducted training for clearance holders on foreign targeting and recruitment and risks of potential foreign influence, Board employees who do not hold a security clearance do not receive this training. Further, multiple DDTRs expressed concerns with employees' lack of awareness of potential risks to personal safety and Board information when traveling internationally. Through available travel data, we were able to determine which divisions and positions typically encounter the highest level of risks most frequently and which divisions appear to be most in need of pretravel briefings for all employees. See the sidebar for our analysis of divisions and positions with the most frequent travel.[6]

DIVISIONS AND POSITIONS WITH THE MOST FREQUENT TRAVEL

Divisions

- International Finance
- Research and Statistics
- Supervision and Regulation
- Monetary Affairs
- Division of Board Members
- Reserve Bank Operations and Payment Systems

Positions

- Principal economist
- Senior economist
- Economic section chief
- Deputy associate director
- Senior special agent

According to the Defense Counterintelligence and Security Agency and ODNI, all federal employees should complete an international travel briefing before official business and unofficial international travel to be aware of the potential risks associated with the planned travel, especially when traveling to high and medium threat locations. Pretravel briefings should include personal safety and potential targeting awareness, information on current travel warnings, and where to seek assistance while abroad.

Beginning in 2023, FRB New York piloted its Threat Awareness and Reporting Operation (TARO) program that provides pretravel briefings and optional post-travel questionnaires to travelers, as well as annual

[5] In addition to training, the Board also offers International SOS services, an international traveler assistance service that provides the Board's international business travelers with general educational training videos on personal and information security risks.

[6] Employees in the divisions and positions with the most travel may have access to sensitive Board information or economic data because of the nature of their work or their seniority.

threat awareness travel briefings for economists and researchers. In 2025, the Division of Reserve Bank Operations and Payment Systems (RBOPS) voluntarily partnered with the TARO program to require pretravel briefings for all RBOPS employees on official business travel or traveling with Board devices to high-risk or restricted countries. In addition, a peer federal financial regulatory agency also provides pretravel briefings and optional post-travel questionnaires for all travelers with a security clearance. National IT also provides researchers with optional National Institute of Standards and Technology security training related to international travel risks.

Through separate conversations with officials in the Division of IT and IINS, we learned that there is no consensus at the Board about which division should lead travel-related briefings. A Division of IT official also stated that there are information classification constraints preventing briefings on certain country-specific travel risks to travelers without a security clearance. In addition, two DDTRs from the six high-travel divisions expressed concern that while Board international travel policies seek to protect Board devices, there are no additional efforts, such as pretravel briefings, that would help protect employees during travel to restricted countries.[7]

INTERNATIONAL TRAVEL RISKS FOR BOARD EMPLOYEES

Foreign intelligence officials often use travel to target members of the U.S. financial sector with information that may further their country's objectives. Below are examples of threats that Board employees should be aware of in restricted countries:

- Cuba's intelligence service uses travel as a method for identifying and interacting with potential targets and often focuses on members of American academia or those with the potential to work in government roles.
- Russian intelligence services conduct spy operations in Mexico to target the United States, as Mexico offers a convenient, lower-risk setting for Russia to oversee U.S. agents and stage other operations.

The Federal Bureau of Investigation states that well planned procedures, including training, travel policies, pretravel briefings, and questionnaires, can help mitigate risks and enhance response times. These procedures could fit into an overall travel risk awareness process.

It is essential for employees to be informed of specific international travel risks that they may face abroad and how to respond to these risks, as evidenced by foreign adversaries' efforts to target U.S. personnel (see sidebar). The Board could leverage existing System unclassified resources from FRB New York's TARO program to better inform Board employees of international travel risks by providing pretravel briefings, threat awareness training, and post-travel questionnaires. Without routine pretravel briefings and threat awareness training, Board employees who do not have a security clearance may lack awareness of international travel risks specific to the agency, potential targeting by foreign entities, personal safety and information security strategies, and country-specific risks. In addition, travelers may not be able to recognize, respond, and report potential risk indicators to safeguard themselves and Board information.

[7] We identified the six divisions with the most international travel by analyzing official business trips and clearance holder business and personal trips from March 1, 2023, to March 31, 2025, in the travel reimbursement platform and clearance holder reporting platform, respectively.

Without post-travel questionnaires, the Board cannot determine whether and when potential suspicious activity has occurred to help mitigate potential security risks for future travelers.

Recommendations

We recommend that the chief operating officer (COO), in conjunction with the information security officer (ISO), leverage existing System resources to

1. Develop and implement a process to provide pretravel briefings covering threat and risk awareness to employees traveling on official business trips or taking Board devices to high-risk and restricted countries, at a minimum.
2. Develop and implement a process to provide Board-specific travel threat awareness trainings for employees in high international travel or senior positions and employees in high traveling divisions, at a minimum.
3. Develop an optional post-travel questionnaire and establish a process to provide the questionnaire to Board employees who are required to report international travel based on the implementation of recommendation 6, at a minimum.

Management Response

In response to our draft report, the COO concurred with the finding and recommendations. Regarding recommendation 1, IINS plans to evaluate training resources and implement threat and risk awareness pretravel briefings before official business travel. IINS plans to address this recommendation by the second quarter of 2027.

Regarding recommendation 2, IINS plans to develop training for all Board employees and offer country-specific training for high-risk destinations. IINS plans to address this recommendation by the fourth quarter of 2026.

Regarding recommendation 3, IINS plans to develop a post-travel questionnaire and work with the ISO to establish a process to provide the questionnaire to affected Board employees. IINS plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

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

Finding 2: The Board Does Not Consolidate and Assess International Travel Data to Identify and Escalate International Travel Risks

We found that the Board does not have a process to internally share travel-related information among relevant Board divisions to aid in identifying and addressing risks and noncompliance with its travel reporting requirements. Specifically, the Board's current analysis of available employee travel data focuses on travel with devices and is not aggregated with other travel data and shared; therefore, centralized trend analysis and threat identification of additional travel risks is not occurring. Leading practices recommend the collection and analysis of available international travel data to identify and share any concerns with an insider risk program. However, the Board's data sources are dispersed among various divisions and information-sharing processes have not been established. Creating a program to consolidate and analyze available international travel data and establishing information sharing processes may allow the Board to centrally identify and mitigate travel risks, as well as assess compliance with its travel reporting requirements.

We identified and analyzed data available to the Board from three sources related to employee international travel from different divisions between March 2023 and March 2025:

1. The Division of IT's Travel Device Request Platform. This platform recorded 3,948 international trips with Board devices,[8] of which approximately 28 percent were to high-risk or restricted countries. While the Division of IT has a process to identify, analyze, and escalate security alerts using data from this platform, it is not always clear when escalations should occur or when analysis suffices to resolve a security alert without any escalation (see sidebar).[9]

DOCUMENTATION OF THE INCIDENT RESPONSE PROCESS

Based on our analysis of the Division of IT's Security Incident Platform, we found that the Division of IT generally analyzes security alerts in accordance with the *Incident Response Manual.* However, the manual can better document circumstances in which additional escalation actions should occur. In the absence of such guidance, escalation occurs at the IT analyst's discretion. Specifically, the manual does not include escalation procedures for alerts related to foreign travel that occurred outside of the reported trip timeline or for data loss protection alerts related to potential removal of FOMC information. In addition, it is unclear how the Division of IT determined that 6 out of 30 security alerts were "false positives," because the manual does not define that term or offer any potential indicators of a typical false positive alert.

[8] International trips with Board devices include business trips, personal trips, and trips that are both business and personal.

[9] We will issue a management alert memorandum for the *Audit of the Board's Offboarding Processes* that includes findings and recommendations related to the Board's information removal response and safeguarding of FOMC information processes. We will also issue a report for the *Evaluation of the Board's Insider Risk Management Activities* that will include additional findings and recommendations related to the Board's insider threat risk management.

2. The Division of Management and Financial Services' Travel Reimbursement Platform. This platform recorded 1,690 international official business trips, of which approximately 19 percent were to high-risk or restricted countries.
3. IINS's Security Clearance Holder Reporting Application. This application recorded 822 business or personal international trips self-reported by security clearance holders, of which approximately 27 percent were to high-risk or restricted countries.

ODNI's *Countering Foreign Intelligence Threats Implementation and Best Practices Guide* recommends the collection of international travel, foreign contact, and foreign visitor information to be automated and retained in a common database or information system to enable trend analysis and threat identification. In addition, SEAD 3 requires clearance holders to report personal international travel and agencies to conduct an analysis of reported activities to determine whether they pose a threat to national security and to take appropriate action. See sidebar for suspicious international travel patterns the Board should monitor. Once an agency identifies concerns that may indicate potential threats, the National Insider Threat Task Force states that agencies should establish repeatable and sustainable processes for information sharing to an insider risk program.

SUSPICIOUS INTERNATIONAL TRAVEL PATTERNS

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

In addition, the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* states that management should identify, analyze, and respond to risks related to achieving its objectives. As such, management should define specific risk tolerances, estimate the significance of any identified risks, and design controls to effectively mitigate the risks. The standards also state that management should communicate relevant and quality information throughout the entity.

While the Board has access to various travel data, the data sources are dispersed among various divisions and information-sharing processes have not been established. For example, the Division of IT can aggregate data from the travel device request platform to identify travel risks related to devices, but these data are neither combined with travel reimbursement or clearance holder reporting travel data nor routinely shared with other divisions. As a result, the Board misses an opportunity to aggregate, monitor, and evaluate enterprisewide employee travel data for potential travel risks beyond travel with devices. Further, the Board is not using available international travel data to assess employees' compliance with travel reporting requirements.

Creating a program that aggregates available international travel data that Board divisions currently obtain from multiple sources may allow the Board to identify and assess broad employee travel patterns to determine which trips and positions present higher levels of travel risks. In addition, consistent information-sharing and clear escalation procedures for travel data can help ensure the Board adequately mitigates and responds to potential threats to Board information or its employees. We believe the Board can benefit from establishing repeatable formalized processes for sharing the patterns and risks found in these aggregated travel records to provide an insider risk program with timely information that can be used to identify risks, analyze and assess potential threats, and resolve incidents.

Recommendation

We recommend that the COO, in conjunction with the ISO,

4. Establish a program that consolidates and assesses international travel data available to Board divisions regarding employee international travel, including

    a. creating capabilities to aggregate and analyze foreign travel data from available sources, including the travel reimbursement platform, the security clearance holder reporting application, and the travel device request platform.

    b. developing a process to reconcile clearance holder unreported travel data.

    c. expanding foreign travel data analysis beyond risks related to travel with devices and developing a process to conduct travel trend analysis including indicators of suspicious travel patterns, define levels of organizational risk tolerances for suspicious travel activity and follow-up processes to understand that activity and escalate any potential threats to the appropriate division and insider risk program, and identify potential travel-related threats that should be factored into training materials.

Management Response

In response to our draft report, the COO concurred with the finding and recommendation. IINS plans to coordinate with the appropriate parties to collect foreign travel data and create a central repository available for analysis and reconciliation of clearance holder unreported travel data. In addition, IINS plans to expand the foreign travel data analysis process to include travel trend analysis and follow-up activities to detect potential threats. Further, IINS also plans to brief divisions about potential travel-related threats. IINS plans to address this recommendation by the first quarter of 2027.

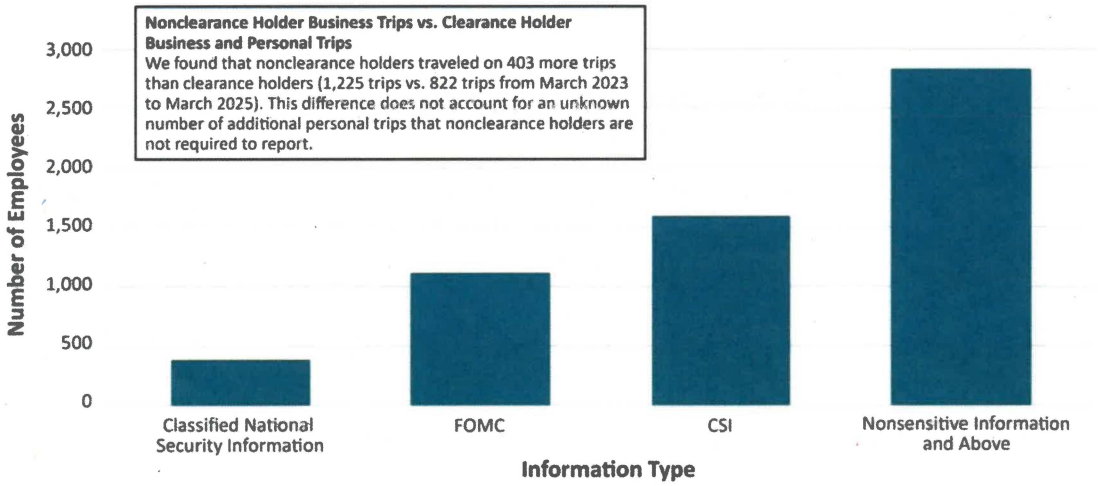
OIG Comment

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

Finding 3: The Board Does Not Require International Travel Reporting for Employees with Access to Sensitive Information

We found that the Board limits its international travel reporting requirements to employees with a security clearance, which represents approximately 12 percent of the Board's workforce.[10] However, some of the Board's most sensitive information, such as FOMC information and CSI, can be accessed by employees who do not have security clearances. We found that 39 percent of the Board workforce can access FOMC information and 56 percent of the Board workforce can access CSI.[11] See figure 6 for a comparison of total Board workforce, who have access to nonsensitive information and above, versus those with access to System sensitive information.

Figure 6. Board Employees, by Information Access Type, as of January 5, 2026



Source: OIG analysis of Human Resource, FOMC, and CSI data. See footnotes 10 and 11.

[10] The percentage of employees with a security clearance is based on security clearance case management system data as of January 2, 2026, and the total number of Board employees as of January 5, 2026, which excludes interns and contractors and includes OIG employees. Security clearances are governed by IINS.

[11] Access to FOMC information and CSI percentages are based on the total number of Board employees as of January 5, 2026; number of employees eligible for FOMC information access as of January 2, 2026; and number of employees eligible for CSI access as of January 3, 2026. FOMC information access is governed by the FOMC Secretariat, and CSI access is governed by the Division of Supervision and Regulation; employees can have access to both sets of information.

[TLP: AMBER+STRICT] [redacted] [U//FOUO] [redacted].[12] A senior Board official informed us that the Board has since implemented several changes related to strengthening the Board's international travel processes.

During outreach, an IINS official told us that the Board has not considered expanding the scope of travel reporting requirements to include positions with access to System sensitive information, such as CSI and FOMC information, but the official believes there may be benefits to doing so. Specifically, the official said that expanding awareness of personal international travel by employees with access to sensitive information may allow the Board to increase its limited insights into the risks presented by such travel. In addition, a DDTR expressed a need to more adequately safeguard FOMC information by automatically restricting an employee's FOMC access when they are traveling to high-risk and restricted countries.

The protection of System information is imperative, as foreign intelligence agents target both U.S. public and private sector financial institutions' employees for sensitive nonpublic information, including FOMC information and CSI. In one instance, for example, the Board was unaware of an employee's personal travel plans to a restricted country, as the employee did not hold a security clearance and was therefore not required to report that personal travel. The employee generated a significant volume of data loss prevention alerts related to removing potentially sensitive documents just before that travel.[13] Without requiring Board employees with access to System sensitive information to report personal international travel in advance, the Board may not become aware of potentially suspicious behaviors before travel, possible travel patterns, and potential threats that employees may face while abroad.

[12] Similarly, a former ranking member of the Senate Committee on Homeland Security and Governmental Affairs issued a report regarding the threat from China to the System and recommended that the System, including the Board, implement robust foreign contact and travel reporting requirements for System employees with access to confidential information, such as FOMC information, to include a compliance and auditing program with penalties for failures to disclose. United States Senate, Committee on Homeland Security and Governmental Affairs, *China's Threat to the Fed: Chinese Influence and Information Theft at U.S. Federal Reserve Banks*, July 2022, https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Report%20-%20China%20Threat%20to%20the%20Fed.pdf, p. *vi*.

[13] We will issue a management alert report related to the Board's offboarding process controls for records management that includes findings and recommendations related to a possible information security incident involving the potential removal of FOMC and other sensitive Board information.

Recommendation

We recommend that the COO

5. Strengthen travel reporting requirements by

    a. determining which Board positions or division employees should be required to report personal international travel before departure based on access to System sensitive information.

    b. updating policies and procedures detailing travel reporting requirements for relevant positions and divisions with access to System sensitive information.

    c. designating a program to monitor reported travel and defining risk monitoring and threat awareness reporting expectations for that program.

Management Response

In response to our draft report, the COO concurred with the finding and recommendation. IINS plans to implement an international travel self-reporting requirement for all employees, update policies and procedures affected by this requirement, and establish an insider risk program to monitor foreign travel. IINS plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

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

Finding 4: The Board Does Not Have a Process to Inform All DDTRs of Travel Risks Before Reviewing Requests for International Travel with Board Devices

While DDTRs generally favor the Division of IT's new *International Travel Risk Decision Guidance*, the guidance is broad and does not have a process to inform all DDTRs of country-specific risks before reviewing and approving employee requests to travel internationally with Board devices. Rather, the Division of IT conducted ad hoc briefings between July 2024 and February 2025 for two of the six high-travel divisions' DDTRs regarding travel to restricted countries. However, three of the six high-travel divisions still expressed a need for more information about the rationale for certain high-risk and restricted countries' risk classifications following the briefings. In addition, two of the six high-travel divisions stated that they were not aware of when or why risk classifications may change. Further, DDTRs from four of the six high-travel divisions informed us that they were not formally trained on the updates to the *International Travel with Mobile Devices Standard*, including the new workflow.

The U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government* describes components and principles that are relevant to establishing effective internal controls for entities to achieve their objectives and mitigate risks, with information and communication being one of the components. In addition, the standard states that management should internally communicate relevant and quality information necessary to support the functioning of the internal control system, as well as provide training to increase awareness of identified risks.

A Division of IT official stated that they focused on ensuring the newly updated workflow process worked properly before providing formal training to the DDTRs and that they provided country-specific risks to DDTRs if they inquired. In addition, DDTRs from three of the six high-travel divisions informed us that they did not receive training because they were already aware of the workflow updates or country risk classifications because of their involvement in the processes of either updating the Division of IT's international travel guidance or determining the countries' risk classifications.

Without established processes to share country-specific risks, not all DDTRs are able to make fully informed decisions concerning the physical and technical risks that could arise from allowing Board employees to travel to foreign countries with their Board devices. Given the evolving and complex geopolitical landscape, understanding the current risks that Board employees may face while abroad in certain countries can better inform DDTRs about whether an employee should travel to the country and what type of Board device the employee should be allowed to use during the international trip. In addition, without timely training on the latest process changes, DDTRs may not be aware of updates to the international travel with Board devices process when reviewing travel requests.

Recommendation

We recommend that the ISO, in conjunction with IINS

6. Develop a process to ensure all DDTRs are informed of country-specific risks at least annually and provide training when updates occur to the international travel with mobile devices process.

Management Response

In response to our draft report, the COO concurred with the finding and recommendation. ISO plans to collaborate with IINS to ensure that DDTRs are provided pretravel briefings as outlined in the management responses for recommendations 1 through 3. The ISO plans to address this recommendation by the fourth quarter of 2026.

OIG Comment

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

Appendix A: Scope and Methodology

To accomplish our objective and to gain an understanding of the Board's process for monitoring international travel, we reviewed Board policies, standards, manuals, and guidance for employee international travel. We also conducted interviews with the Office of the Chief Operating Officer, Division of IT, the Board's economics divisions (Divisions of Financial Stability, International Finance, Monetary Affairs, and Research and Statistics), and other divisions with frequent travelers.

We identified the six divisions with the most international travel by analyzing official business trips and clearance holder business and personal trips from March 1, 2023, to March 31, 2025, in the travel reimbursement platform and clearance holder reporting platform, respectively. Our analysis of travel data is based on the Board's organizational structure and division names during our review period and does not reflect organizational restructuring conducted after March 31, 2025.

We reviewed relevant directives and identified applicable criteria from multiple federal agencies. Our sources include ODNI, the U.S. Department of State, Defense Counterintelligence and Security Agency, the Federal Bureau of Investigation, National Institute of Standards and Technology, U.S. Chief Information Officers Council, the United States Senate, and the U.S. Government Accountability Office. Further, we interviewed staff from one peer federal financial agency, FRB New York, and National IT to identify leading practices related to monitoring processes for international travel.

To analyze Board employees' international travel, we obtained data from the following sources:

- **Travel Reimbursement Platform.** (March 1, 2023, to March 31, 2025) Board employees and supervisors use this platform to create and approve travel authorizations and travel expenses for reimbursement. This platform is used for all official Board travel and reimbursements, regardless of the employee's security clearance status.

- **Clearance Holder Reporting Application.** (March 1, 2023, to March 31, 2025) Board employees with national security clearance use this web application to self-report international travel, including official business and personal travel.

- **Travel Device Request Platform.** (March 1, 2023, to March 31, 2025) Board employees and supervisors use this platform to request and approve international travel with Board devices, including official business and personal travel.

- **Security Incident Platform.** (February 1, 2025, to March 31, 2025) The Division of IT uses this platform to identify suspicious activity and triage potential incidents, including security incidents while travelers are abroad. We judgmentally selected a sample of 30 out of 130 security alerts related to international travel to determine whether the Division of IT follows its documented incident response procedures.

- **Human Resource System.** (as of April 3, 2025, and January 5, 2026) The Board uses this system to centralize human resource employee data.

- **Case Management System.** (as of August 1, 2025, and January 2, 2026) The Board uses this system to track personnel suitability, security clearance investigations, and adjudications.

Our analysis of these data sources was to (1) determine the divisions, countries, and positions with the most travel; (2) reconcile clearance holder reported travel with official business travel; and (3) assess the Division of IT's incident response process.

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

Appendix B: International Travel Guidance

We analyzed the following frameworks and guides to identify additional strategies the Board could implement to enhance its protection of its information and people.

- ODNI's SEAD 3 mandates international travel reporting requirements for all individuals who have access to classified information or hold a sensitive position and states that (1) agencies shall analyze reported travel activities, (2) individuals may receive pretravel briefings, and (3) agencies shall provide training on travel reporting obligations.

- The Defense Counterintelligence and Security Agency issued the *SEAD 3 Job Aid: Unofficial Foreign Travel Reporting and Activities Checklist*, which provides recommendations for pretravel briefings and the reporting of any contact with foreign intelligence entities or foreign personnel, travel anomalies, and deviations from the reported travel itinerary.

- ODNI's *Countering Foreign Intelligence Threats Implementation and Best Practices Guide* establishes best practices for strengthening protective programs and reducing foreign intelligence risks. The guide recommends (1) requiring personal travel reporting, (2) providing pretravel and post-travel briefings on high and medium threat locations, (3) analyzing travel information to safeguard sensitive information, and (4) sharing threat and vulnerability information.

- The National Insider Threat Task Force's *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards* focuses on insider threat program optimization, stating that agencies shall provide insider threat programs with timely information, such as travel records and foreign contact reports, to identify, analyze, and resolve insider threats.

- Defense Counterintelligence and Security Agency's *Foreign Travel Brief Short Student Guide* is a template for creating pretravel briefings and post-travel questionnaires on international travel vulnerabilities. The guide states that employees should complete a pretravel briefing to learn about international travel risks and receive a post-travel questionnaire related to potentially concerning travel activities.

- The National Institute of Standards and Technology's *Safeguarding International Science Research Security Framework* establishes best practices for safeguarding international science while mitigating risks to an open collaborative environment. The framework states that annual research security training should be provided to employees, including foreign interference or influence and employee responsibilities related to safeguarding international science as determined by the organization.

Appendix C: Management Response

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

OFFICE OF THE
CHIEF OPERATING OFFICER

May 27, 2026

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

Dear Mr. VanHuysen:

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report titled *The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks*. We appreciate the OIG's effort to develop the report and recommendations to further strengthen the Board's programs and processes governing employees who travel abroad.

We are proud of the work accomplished by our Information Security (IS) and Intelligence, Insider Risk, and National Security Programs (IINS) teams. We realize we have additional work to enhance educating employees about identifying and mitigating international travel risks, collecting, consolidating and analyzing travel data, and sharing travel information and risks with Board groups when appropriate.

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 foreign travel programs and processes. We look forward to continued work with your office in the future.

Regards,

WINONA VARNON

Digitally signed by WINONA VARNON
Date: 2026.06.02 13:10:50 -04'00'

Winona H. Varnon

www.federalreserve.gov

cc:

Jeff Reidel
Rendell Jones
Chip Young
Tannaz Haddadi
Amy Kelley
Jeffrey Dawson
Kelly Gibbs
Melissa Catterall
Leah Middleton
Linda Comilang

Response to recommendations presented in the Draft OIG Report,

"The Board Can Strengthen Its Process to Monitor and Mitigate International Travel Risks"

Finding 1: The Board Should Better Inform Employees of International Travel Risks

We recommend that the chief operating officer (COO), in conjunction with the information security officer (ISO), leverage existing System resources to:

Recommendation 1: Develop and implement a process to provide prebriefs covering threat and risk awareness to employees traveling on official business trips or taking Board devices to high-risk and restricted countries, at a minimum.

Management Response:
We concur with the finding and recommendation. IINS is evaluating available training resources and will implement threat and risk awareness pre-briefs to employees prior to traveling on official business. Target Date: Q2 2027.

Recommendation 2: Develop and implement a process to provide Board-specific travel threat awareness trainings for employees in high international travel or senior positions and employees in high traveling divisions, at a minimum.

Management Response:
We concur with the finding and recommendation. IINS will develop training for all Board employees and offer country specific training for high risk destinations. Target Date: Q4 2026.

Recommendation 3: Develop an optional post-travel questionnaire and establish a process to provide the questionnaire to Board employees who are required to report international travel based on the implementation of recommendation 6, at a minimum.

Management Response:
We concur with the finding and recommendation. IINS will develop a post-travel questionnaire for Board employees and identify the appropriate population to complete the questionnaire. In addition, IINS will work with the ISO to establish a process to provide the questionnaire to affected Board employees. Target Date: Q4 2026.

Finding 2: The Board Does Not Consolidate and Assess International Travel Data to Identify and Escalate International Travel Risks

We recommend that the COO, in conjunction with the ISO,

Recommendation 4: Establish a program that consolidates and assesses international travel data available to Board divisions regarding employee international travel, including

a. creating capabilities to aggregate and analyze foreign travel data from available sources, including the travel reimbursement platform, the security clearance holder reporting application, and the travel device request platform.

b. developing a process to reconcile clearance holder unreported travel data.

c. expanding foreign travel data analysis beyond risks related to travel with devices and developing a process to conduct travel trend analysis including indicators of suspicious travel patterns, define levels of organizational risk tolerances for suspicious travel activity and follow-up processes to understand that activity and escalate any potential threats to the appropriate division and insider risk program, and identify potential travel-related threats that should be factored into training materials.

Management Response:
We concur with the finding and recommendation. IINS will coordinate with the appropriate parties (e.g., the Board's Security Operations Center and the Travel group) to collect foreign travel data to create a central repository so that that information is readily available for analysis and other related purposes. Target Date: Q4 2026.

Regarding recommendation 4b, as part of the effort to create the central repository, a process to reconcile clearance holder unreported travel data will be included and will begin once the repository is operational. Target Date: Q1 2027.

For recommendation 4c, IINS will collaborate with the appropriate parties to expand the current foreign travel data analysis process. This will include adding travel trend analysis and follow-up activities to understand activity and detect potential threats. Additionally, divisions would be briefed about potential travel-related threats via the foreign travel and the threat awareness briefs. Target Date: Q1 2027.

Finding 3: The Board Does Not Require International Travel Reporting for Employees with Access to Sensitive Information

Recommendation 5: Strengthen travel reporting requirements by

a. determining which Board positions or division employees should be required to report personal international travel prior to departure based on access to Federal Reserve System sensitive information.

b. updating policies and procedures detailing travel reporting requirements for relevant positions and divisions with access to Federal Reserve System sensitive information.

c. designating a program to monitor reported travel and defining risk monitoring and threat awareness reporting expectations for that program.

Management Response:
We concur with the finding and recommendation. IINS will implement a Board-wide policy to require self-reporting of international travel by all employees. Target Date: Q4 2026.

In addition, to satisfy recommendation 5b, IINS will coordinate with the appropriate Board groups to update current travel and security policies and procedures affected by the adoption of this requirement. Target Date: Q4 2026.

Regarding recommendation 5c, IINS will establish a robust insider risk program that will monitor foreign travel. Target Date: Q4 2026.

Finding 4: The Board Does Not Have a Process to Inform All DDTRs of Travel Risks Prior to Reviewing Requests for International Travel with Board Devices

Recommendation 6: Develop a process to ensure all DDTRs are informed of country-specific risks at least annually and provide training when updates occur to the international travel with mobile devices process.

Management Response:
We concur with the finding and recommendation. The ISO will collaborate with IINS to ensure that DDTRs are provided the travel prebriefs as outlined in the management responses for recommendations 1 through 3 in this memo. Target Date: Q4 2026.

Abbreviations

COO	chief operating officer
CSI	confidential supervisory information
DDTR	division designated travel reviewer
FOMC	Federal Open Market Committee
FRB New York	Federal Reserve Bank of New York
IINS	Intelligence, Insider Risk, and National Security Programs
ISO	information security officer
National IT	Federal Reserve Information Technology
ODNI	Office of the Director of National Intelligence
RBOPS	Division of Reserve Bank Operations and Payment Systems
SEAD	Security Executive Agent Directive
TARO	Threat Awareness and Reporting Operation

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

Hotline

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

oig.federalreserve.gov/hotline

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

1-800-827-3340

General Contact Information

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

202-973-5000

Media and Congressional Inquiries

oig.media@frb.gov