TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

IRS Employees' Unauthorized Use of Mobile Devices Overseas

May 18, 2026

Report Number: 2026-IE-R008

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: IRS Employees' Unauthorized Use of Mobile Devices Overseas

Final Evaluation Report issued on May 18, 2026 **Report Number 2026-IE-R008**

Why TIGTA Did This Evaluation

We initiated this evaluation in response to media coverage involving federal employees who took their government-furnished mobile devices abroad without authorization. Employees taking their devices abroad is an inherent security challenge; however, enhanced controls can minimize this risk and protect sensitive data.

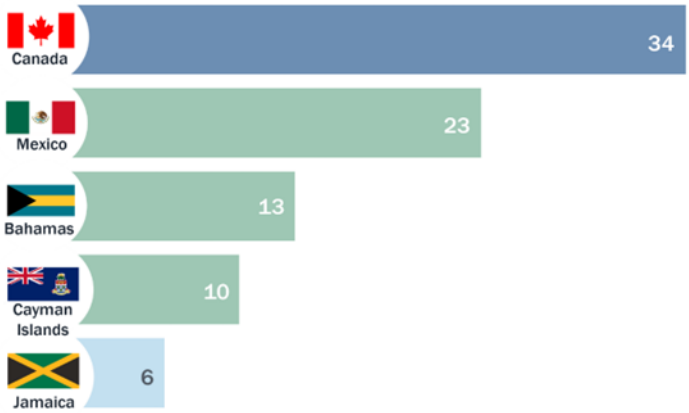
The overall objective of this evaluation was to assess the IRS's efforts to prevent the unauthorized use of mobile devices in foreign countries.

Impact on Tax Administration

Foreign adversaries seeking confidential, intellectual, and sometimes personal data often target federal government employees. Without appropriate safeguards, foreign adversaries can steal and exploit sensitive or classified information on federal employees' mobile devices. Foreign adversaries can also use compromised mobile devices to attack federal government computer networks.

What TIGTA Found

We reviewed the IRS's Fiscal Year (FY) 2024 mobile device usage reports for smartphones and tablets. We identified 173 instances of IRS employees' mobile devices connecting to a foreign cellular network without a corresponding travel authorization to use their work equipment overseas. The connections were associated with 121 employees in 37 countries, spanning 5 continents. The top five countries for unauthorized foreign connections in FY 2024 were:



IRS policies prohibit employees from taking government-furnished mobile devices overseas for any personal or official travel, unless employees receive approval in advance. However, the potential exists for IRS employees to take and use the following devices overseas without authorization:

- Government-furnished mobile hotspots, laptops, smartphones, and tablets.
- Nongovernment issued, personally owned mobile devices approved through the IRS's Bring Your Own Device program.

The mobile phone vendor provides the IRS with monthly reports for devices with foreign connections, but the IRS does not monitor these reports for international use. Instead, the IRS only monitors the monthly reports to confirm charges were authorized.

IRS officials request authorization to bring government-furnished mobile devices on international travel using Form 1321, *Authorization for Official Travel.* The form must be uploaded on all employees' travel vouchers. This form is useful for determining when an employee is traveling overseas. However, the form does not track specific mobile devices being taken overseas to determine whether the devices should be sanitized and reimaged after returning to the United States.

What TIGTA Recommended

We recommended that the IRS implement a process to review vendor usage reports for overseas mobile device activity and to update Form 1321 to include the name and other identifiable features of mobile devices being taken outside the country. The IRS agreed with both recommendations.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: May 18, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Nancy A LaManna
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – IRS Employees' Unauthorized Use of Mobile Devices Overseas (Evaluation No.: IE-25-017)

This report presents the results of our review to assess the IRS's efforts to prevent the unauthorized use of mobile devices in foreign countries. This evaluation is part of our Fiscal Year 2026 Annual Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Frank O'Connor, Director.

Table of Contents

Background

Foreign adversaries seeking confidential, intellectual, and sometimes personal data often target federal government employees. Without appropriate safeguards, foreign adversaries can steal and exploit sensitive or classified information on federal employees' mobile devices. Foreign adversaries can also use compromised mobile devices to attack federal government computer networks.

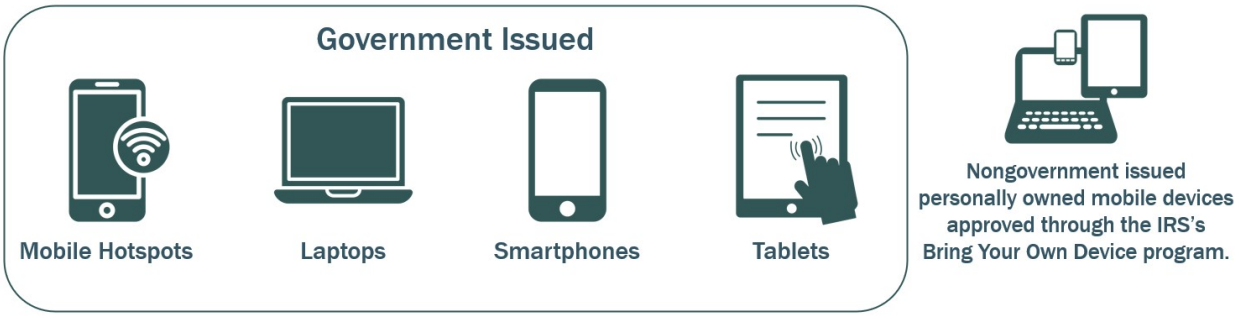
Mobile devices, such as smartphones and tablets, allow federal employees to fulfill work-related responsibilities outside of an office. While these devices provide telecommunications capabilities, connectivity to information systems, and work-related applications, they also have software and hardware vulnerabilities.

A foreign adversary successfully exploiting a federal worker's mobile device could remotely activate microphones and cameras, and geolocate and track other devices. They also could steal information processed by or stored on a worker's mobile device.

As of October 2025, the Internal Revenue Service (IRS) had nearly 99,000 government-furnished devices assigned to employees, including nearly 87,000 computers and more than 12,000 mobile phones and tablets. Employees can have multiple devices assigned to them. IRS policies generally prohibit employees from taking government-furnished mobile devices overseas for any personal or official travel, unless employees receive approval in advance.

The Chief Information Security Officer, or designee, must give written approval before an individual may take a government-owned computer and/or other mobile device overseas. The Department of the Treasury defines "overseas" as "any area situated outside the United States." The term "United States" includes the District of Columbia, the Commonwealth of Puerto Rico, and the possessions of the United States (excluding the Trust Territory of the Pacific Islands and Midway Island). IRS employees could potentially take and use the following devices overseas without authorization:[1]

Figure 1: Digital Options Available in the FY 2024 IRS Mobile Device Program



Source: TIGTA's analysis of the IRS's FY 2024 mobile device program.

According to IRS Cybersecurity Operations, the Computer Security Incident Response Center's (CSIRC) Security Operations Center (SOC) is responsible for monitoring mobile devices overseas.

[1] The BYOD program allows IRS personnel to use nongovernment furnished, personally owned mobile devices for business purposes.

The SOC identifies, tickets, and remediates situations when a government-furnished mobile or a Bring Your Own Device (BYOD) attempts to access IRS systems from overseas. The SOC considers all overseas connections unauthorized, unless the CSIRC has received prior notification and appropriate approvals are in place.

Unauthorized IRS mobile devices can access the IRS network. However, once the device is detected and identified as a connection originating from overseas, the SOC tickets the device and terminates the connection. The unauthorized mobile device is denied access to the IRS network until it has been sanitized and reimaged.[2]

After the SOC tickets an unauthorized mobile device, the Cybercrime Unit within TIGTA's Office of Investigations should be notified about the incident. The employee's direct supervisor and chain of command are also notified. The CSIRC instructs the supervisor to obtain a written statement from the employee about the details of the incident. Reported incidents are documented in a centralized incident-tracking system. Incidents are also assessed to determine the validity, severity, and impact of the event, as well as any legal or criminal consequences.

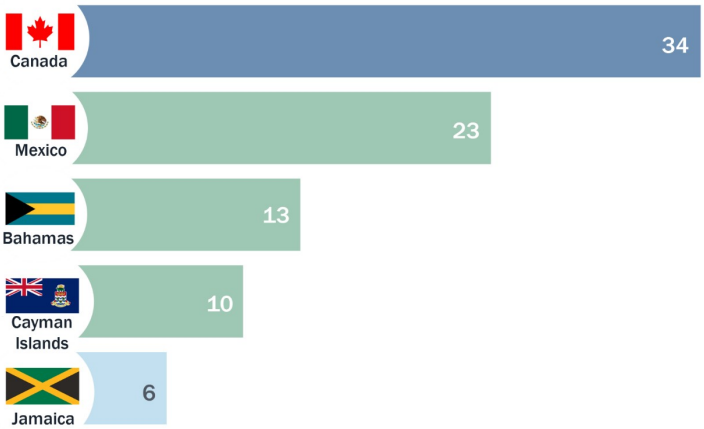
Results of Review

We initiated this evaluation in response to recent media accounts where other federal agency employees took their government-furnished mobile devices abroad and used them without authorization. We found concerns with the controls in place to identify employees potentially transporting their government-furnished mobile devices without authorization abroad. Our analysis of IRS mobile device usage reports for FY 2024 identified at least 173 instances where employees transported their government-furnished mobile devices abroad.[3] These instances involved employees that did not receive advanced approval to travel and connected to a foreign cellular network. However, the CSIRC was not alerted to any policy violation. Without additional controls, IRS devices are at risk of unauthorized access and susceptible to cyberattacks. Further, the IRS does not have a process to accurately distinguish which devices are being taken abroad once an employee is approved for travel.

[2] The sanitization process removes information from the media. The information cannot be retrieved or reconstructed. Sanitization techniques include clearing, purging, cryptographic erase, and destruction. Reimaging is the process of removing all software on a device and reinstalling the removed software.

[3] The IRS's fiscal year runs from October 1 to September 30.

Figure 2: Top Five Countries for Unauthorized Foreign Connections in FY 2024



Source: TIGTA's analysis of IRS mobile device usage reports.

The IRS Did Not Identify Some Mobile Devices Taken Overseas

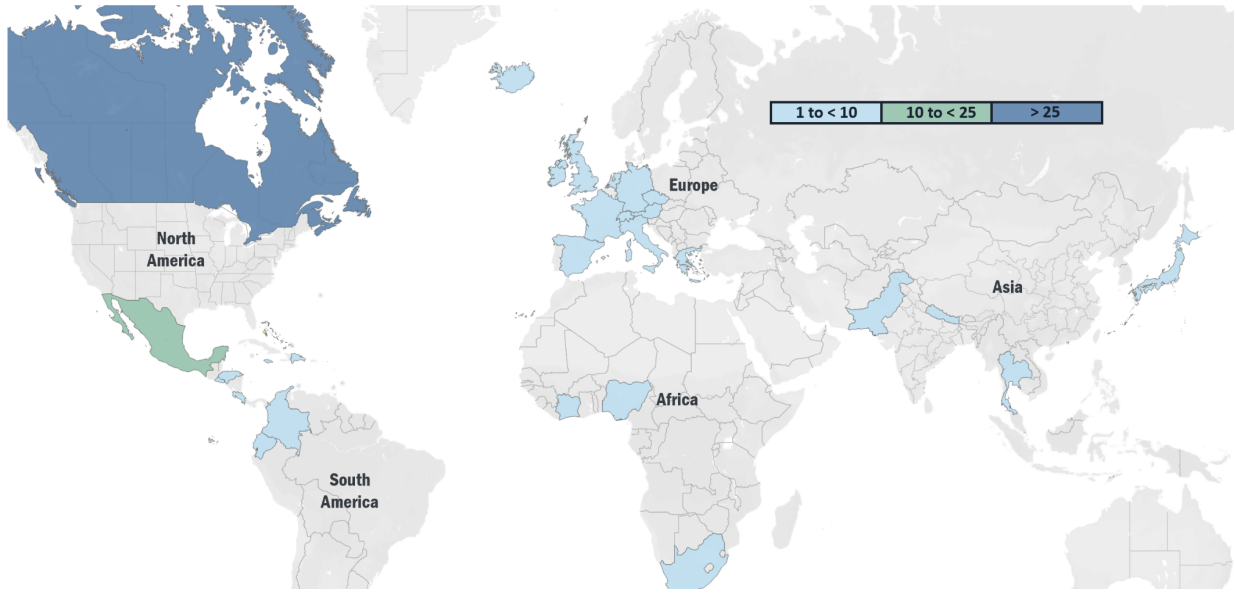
We reviewed the IRS's FY 2024 mobile device usage reports for smartphones and tablets. These reports had a total of 4,066 potential overseas connections. We then compared these connections to official travel and mobile device authorization records. In FY 2024, there were at least 173 instances of IRS employees' mobile devices connecting to a foreign cellular network without corresponding travel authorizations to use their work equipment overseas.[4] The connections were associated with 121 employees in 37 countries, spanning 5 continents.[5]

We were able to identify mobile devices taken overseas by searching for roaming text messages, roaming voice, and data charges and use. Figure 3 shows the different foreign countries where IRS employees used their mobile devices and the number of connections in each country.

[4] We identified connections to foreign networks. Some foreign network connections were in Canada and Mexico and occurred near the residences of employees. We considered these instances to be "accidental" and excluded them. We also excluded connections that appear to have happened enroute to or returning from official travel destinations.

[5] Additionally, 20 devices connected to an "unknown" country. For example, some devices connected to a network in international waters. Appendix II provides a full list of the countries.

Figure 3: Location of Unauthorized Foreign Connections in FY 2024



Source: TIGTA's analysis of IRS mobile device usage reports.

Unless approved in advance, IRS employees are prohibited from taking government-furnished mobile devices overseas during personal or official travel. The Chief Information Security Officer or designee must give written approval before an employee can take a government-owned computer and/or other mobile device overseas. Risks associated with using mobile devices overseas include their ability to potentially connect to any available network, including untrusted wireless networks or foreign cellular networks.

In Calendar Year 2024, the IRS began providing loaner phones for international service. The loaner phone program was established because IRS executives did not want their phones wiped when they returned. This program was then extended to all IRS personnel traveling internationally. IRS employees request authorization to bring government-furnished mobile devices on international travel using Form 1321, *Authorization for Official Travel.* The approved form must be uploaded with the voucher in the IRS's travel system.

According to the IRS, they can identify overseas use when an employee accesses an IRS system or application. However, the IRS cannot identify casual use, such as accessing a map application or searching the internet. The IRS noted that even though employees can connect to foreign cellular networks, international cellular service should be blocked on all mobile devices. These situations pose additional threats because the IRS does not know whether a device needs to be sanitized or reimaged.

The mobile phone vendor provides the IRS with monthly reports for devices with foreign connections, but the IRS does not monitor the reports for international use.[6] Instead, the IRS only monitors the monthly reports to confirm charges were authorized. The User and Network Services (UNS) reported that the vendor has shown incorrect data in the past. However, the UNS has not found any issues with international data.

[6] We limited our analysis to mobile devices that the IRS's largest cell phone contractor services.

When a device accesses the IRS network, this can trigger a "risky user" alert for analysts to review. The alerts cause the system to block the account. In addition, accessing common applications like email and files is restricted until the Office of Information Technology security personnel review and remediate the alert. The following situations can cause a "risk user" alert:

- **Impossible Travel**: The network detects a device's location is in multiple places during a short period of time, it may flag the device for impossible travel.

  Example: Analysts may see connections to Estonia within 20 or 30 minutes of a prior United States location. They can view Enterprise Remote Access Project data to determine where the device was physically located. In this scenario, a ticket will be closed as a "non-incident."

- **Unusual Login**: The IRS network detects a user signing into a government-furnished or BYOD device under unusual circumstances. The IRS cannot stop an employee from taking their personal devices overseas. However, if an employee tries to access email while overseas, the system will flag this as a risky user.

In FY 2024, the IRS noted that there were 103 "risky user" alerts from employees who used a tablet, cell phone, or BYOD overseas. The IRS stated that only one was unauthorized. However, the IRS did not provide complete details on the violation identified. They only noted that violation did not include overseas usage.

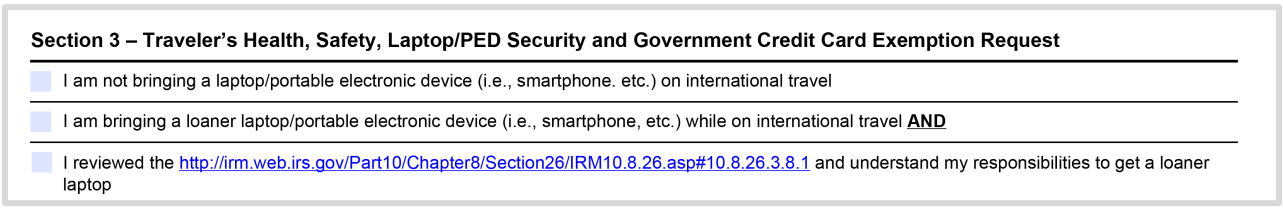
We confirmed the IRS did not have a process to compare all mobile device usage against official travel records. Further, we determined international usage could not have been blocked across all IRS mobile devices as previously indicated by the IRS. During our review, the IRS acknowledged potential instances where international blocks expired, allowing temporary access for employees to send and receive international communications. To address and prevent this, the IRS implemented a control to perform a more comprehensive review of usage reports and ensure blocks remain active on every line.

Changes to overseas travel form could help identify unauthorized devices

The IRS also does not have a process to accurately track and identify which mobile devices are taken overseas. For example, Form 1321 does not specifically list what device(s) the employee is allowed to bring or what country they are traveling to. The form only captures whether an employee is or is **NOT** bringing a laptop/portable electronic device on international travel.

Form 1321 is useful for determining when an employee is traveling overseas. However, the form does not track specific mobile devices being taken overseas to determine whether the devices should be sanitized and reimaged after returning to the United States. IRS Cybersecurity officials indicated that documenting the type of device would be helpful. Figure 4 shows an excerpt of the information found on Form 1321.

Figure 4: Excerpt of Form 1321, *Authorization for Official Travel*



Section 3 – Traveler's Health, Safety, Laptop/PED Security and Government Credit Card Exemption Request

☐ I am not bringing a laptop/portable electronic device (i.e., smartphone. etc.) on international travel

☐ I am bringing a loaner laptop/portable electronic device (i.e., smartphone, etc.) while on international travel **AND**

☐ I reviewed the http://irm.web.irs.gov/Part10/Chapter8/Section26/IRM10.8.26.asp#10.8.26.3.8.1 and understand my responsibilities to get a loaner laptop

Source: IRS Form 1321, Authorization for Official Travel, Section 3.

IRS Cybersecurity currently compares suspicious activity alerts received from an employee's device against a travel "exception list" that a separate IRS function maintains. Cybersecurity analysts determine whether to restrict further access by verifying the individual is on the "exception list." However, the analysts do not know whether a device was approved for travel.

Additionally, IRS officials stated that some approval processes are not properly documented. When an employee files a request to travel abroad, the UNS is responsible for fulfilling the request. However, the UNS is not provided with any later changes that might occur through an employee's chain of command. For example, the UNS would not know whether the travel area or the authorization period was modified beyond the original dates listed on Form 1321. The UNS noted that in one instance, an employee was authorized to work in a foreign country due to the COVID-19 pandemic. This authorization was given to the employee via email, but there were no official forms documenting the approval process.

Updating Form 1321 to include additional information, such as the approved device and type, could help the IRS maintain accurate records. Having additional information on the form will also help document whether a device was returned and sanitized, and help identify unauthorized overseas use. With more specific information, the Office of Information Technology can provide better support for employees approved to travel abroad. Employees taking their devices abroad is an inherent security challenge; however, enhanced controls can minimize this risk and protect sensitive data.

The Chief Information Officer should:

Recommendation 1: Implement a process to review vendor usage reports for overseas mobile device activity. Further, take appropriate actions to sanitize the devices transported overseas in accordance with existing IRS procedures.

> **Management's Response:** The IRS agreed with this recommendation and will implement a process to review vendor usage reports for overseas mobile device activity and ensure appropriate actions are taken to sanitize devices transported overseas in accordance with IRS policy.

Recommendation 2: Update Form 1321 to include the name and other identifiable features of mobile devices being taken outside the country.

> **Management's Response:** The IRS agreed with this recommendation and will update Form 1321 to include an area to document asset tracking information about mobile devices being taken outside the country.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this project was to assess the IRS's efforts to prevent the unauthorized use of mobile devices in foreign countries. To accomplish our objective, we:

- Interviewed appropriate IRS officials and reviewed IRS policies and procedures to gain an understanding of how the IRS monitors government-furnished smartphones and tablets taken on international travel without authorization. We limited the scope of our review to procedures that involve:
    - Requesting, approving, and documenting approval to take government-issued mobile devices (phones and tablets) on international travel.
    - Identifying mobile devices that have been used internationally without authorization and securing these devices after unauthorized international travel.
- Analyzed FY 2024 monthly usage reports for smartphones and tablets to identify any instances where data was used, messages were sent, or calls were made internationally without authorization. When conducting our analysis, we:
    - Validated FY 2024 usage reports and compared these reports to an employee's official travel information to determine whether there was a valid travel authorization for the dates an employee traveled with an approved Form 1321.
    - Obtained a list of approved FY 2024 international travelers to match against usage reports and confirmed the employees traveled with an approved Form 1321. We also:
        - Eliminated potential exceptions due to "Impossible Travel" or employees who reside/visit areas where accidental connections could likely occur.
        - Analyzed employees' official travel records and Discovery Directory to observe whether travel to a foreign country would have been possible or the likelihood for connection to a foreign tower exists.
    - Identified a sample of employee smartphones and tablets to validate usage reports against billing information from the contractor. This was done to ensure the accuracy of usage report data.

Performance of This Review

This review was performed with information obtained from IRS Travel Management, Cybersecurity, and the UNS from November 2024 through September 2025. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Data Validation Methodology

We performed tests to assess the reliability of mobile device usage reports. We evaluated the data by (1) performing tests on device usage data against source documentation from mobile device vendors; (2) reviewing existing information about device usage data and the vendor that produced the data; and (3) interviewing agency officials knowledgeable about device usage data. We determined that the data were sufficiently reliable for purposes of this report.

Appendix II

Countries With Unauthorized Mobile Device Connections in Fiscal Year 2024

Aruba	Hong Kong
Austria	Iceland
Bahamas	Ireland
Barbados	Italy
Bermuda	Jamaica
Canada	Japan
Cayman Islands	Luxembourg
Colombia	Mexico
Costa Rica	Nepal
Cote D'Ivoire	Netherlands
Czech Republic	Nigeria
Dominican Republic	Pakistan
Ecuador	South Africa
El Salvador	Spain
France	Switzerland
Germany	Thailand
Greece	Turks and Caicos Islands
Grenada	United Kingdom
Honduras	

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

April 30, 2026

MEMORANDUM FOR NANCY A. LAMANNA
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS

FROM: Kaschit Pandya
Chief Information Officer

Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2026.04.30 09:02:44 -04'00'

SUBJECT: Draft Evaluation Report – IRS Employees' Unauthorized Use of Mobile Devices Overseas (Evaluation #IE-25-017)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. The IRS has taken and will continue to take steps to monitor use of mobile devices overseas to prevent unauthorized use. The IRS remains committed to continuous improvement consistent with established policies and guidelines.

Management agrees with the recommendations and will take appropriate actions to address the identified issues and improve our use of mobile devices overseas. Please refer to the attachment for specific details.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact me at (202) 315-5000, or a member of your staff may contact Tanya Chiaravalle, Coordinating Director, End User Digital Services, at (240) 613-4255.

Attachment

Attachment

Evaluation # IE-25-017, IRS Employees' Unauthorized Use of Mobile Devices Overseas

Recommendations

RECOMMENDATION 1: The Chief Information Officer should implement a process to review vendor usage reports for overseas mobile device activity. Further, take appropriate actions to sanitize the devices transported overseas in accordance with existing IRS procedures.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will implement a process to review vendor usage reports for overseas mobile device activity and ensure appropriate actions are taken to sanitize devices transported overseas in accordance with IRS policy.

IMPLEMENTATION DATE: July 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

RECOMMENDATION 2: The Chief Information Officer should update Form 1321 to include the name and other identifiable features of mobile devices being taken outside the country.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will update Form 1321 to include an area to document asset tracking information about mobile devices being taken outside the country.

IMPLEMENTATION DATE: July 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, End User Digital Services

Appendix IV

Abbreviations

BYOD	Bring Your Own Device
CSIRC	Computer Security Incident Response Center
FY	Fiscal Year
IRS	Internal Revenue Service
SOC	Security Operations Center
TIGTA	Treasury Inspector General for Tax Administration
UNS	User and Network Services

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.