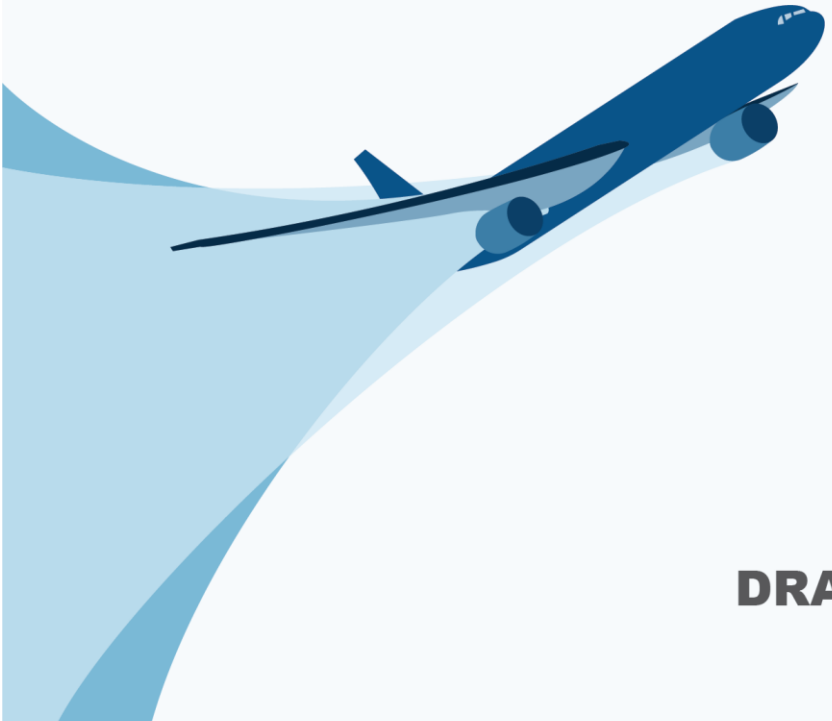
Federal Mobility Group (FMG)

# INTERNATIONAL TRAVEL GUIDANCE

## for Government Mobile Devices



DRAFT

August 2021

# Acknowledgements


- Department of Homeland Security
- Department of Homeland Security – Science & Technology (S&T)
- Department of Homeland Security - Cybersecurity Infrastructure Security Agency (CISA)
- State Department
- Department of Education
- Department of Energy
- Department of Defense (DOD)
- Department of Interior (DOI)
- Department of Treasury
- General Services Administration (GSA)
- National Aeronautics and Space Administration (NASA)

# Executive Summary

Mobile devices have evolved to become the critical link between a remote user and their home office, providing travelers access to business applications and data they would otherwise lack. Ensuring that this line of communication is private and secure is imperative. The security guidance herein applies to U.S. Government personnel, detailees, or contractors using Government-furnished commercial mobile devices (Government Furnished Equipment [GFE]) in a public network as they travel to, from, and within foreign countries. The purpose of this report is to minimize an adversary's ability to obtain sensitive data through GFE mobile devices and limit damage should a device be compromised. The mitigations address a range of threats that might be encountered in foreign countries along with best practice mitigations.

Mobile devices have inherent vulnerabilities associated with their software and hardware. Foreign countries often leverage their security apparatus—especially airport security, customs, and connections to the tourism industry—to conduct physical attacks on mobile devices. Also, in many foreign countries the government has direct or proxy control of the commercial cellular infrastructure, which gives them a remote conduit to attack connected mobile devices. Cellular-borne attacks are particularly damaging, as most mobile devices—by design—trust the signaling/management communications from a cellular network.

Successful exploitation can allow adversaries to remotely activate microphones and cameras, geolocate and track specific devices, and steal the information processed by or stored on the device. A compromised device can also be used as a vector to attack connected enterprise networks. High-profile U.S. Government personnel are top targets and if a mobile device is required while they are traveling overseas, they should carry or employ a disposable or loaner commercial mobile device for travel in high-threat environments. They should not carry their Government-furnished mobile device in these high-threat environments

For those personnel who require unclassified official government-issued, commercial mobile devices when traveling outside the continental U.S. (OCONUS) and its territories, certain countermeasures can be employed to mitigate some of the vulnerabilities. Foreign embassies and consulates are also considered foreign territory, regardless of location, and therefore the recommended mitigations in this guidance document also apply to personnel traveling to embassies or consulates located in the U.S. Personal devices used to conduct official business during international travel are outside the scope of this document, however, the threats outlined are also applicable to personal devices. As such, users should consider protective countermeasures similar to those described herein when traveling with personal devices and conducting government duties on those devices while on travel.

The guidance outlines best practices regarding configuration and use of GFE mobile devices to safeguard information, backend enterprise systems, and users while on international travel. It includes sample checklists for pre, during, and post travel, and outlines considerations for border crossings and access to secured areas while on foreign travel. Agencies can use the procedures and best practices described in this document to develop agency-specific policy based on their risk tolerance.

The guidance considerations are drawn from documents developed by the following federal agencies: the Department of Homeland Security (DHS), Department of State (State), Department of Defense (DoD), and National Security Agency (NSA), as referenced herein.

Figure 1. summarizes general risk mitigations from Mobile Device Best Practices When Traveling OCONUS published by the NSA.

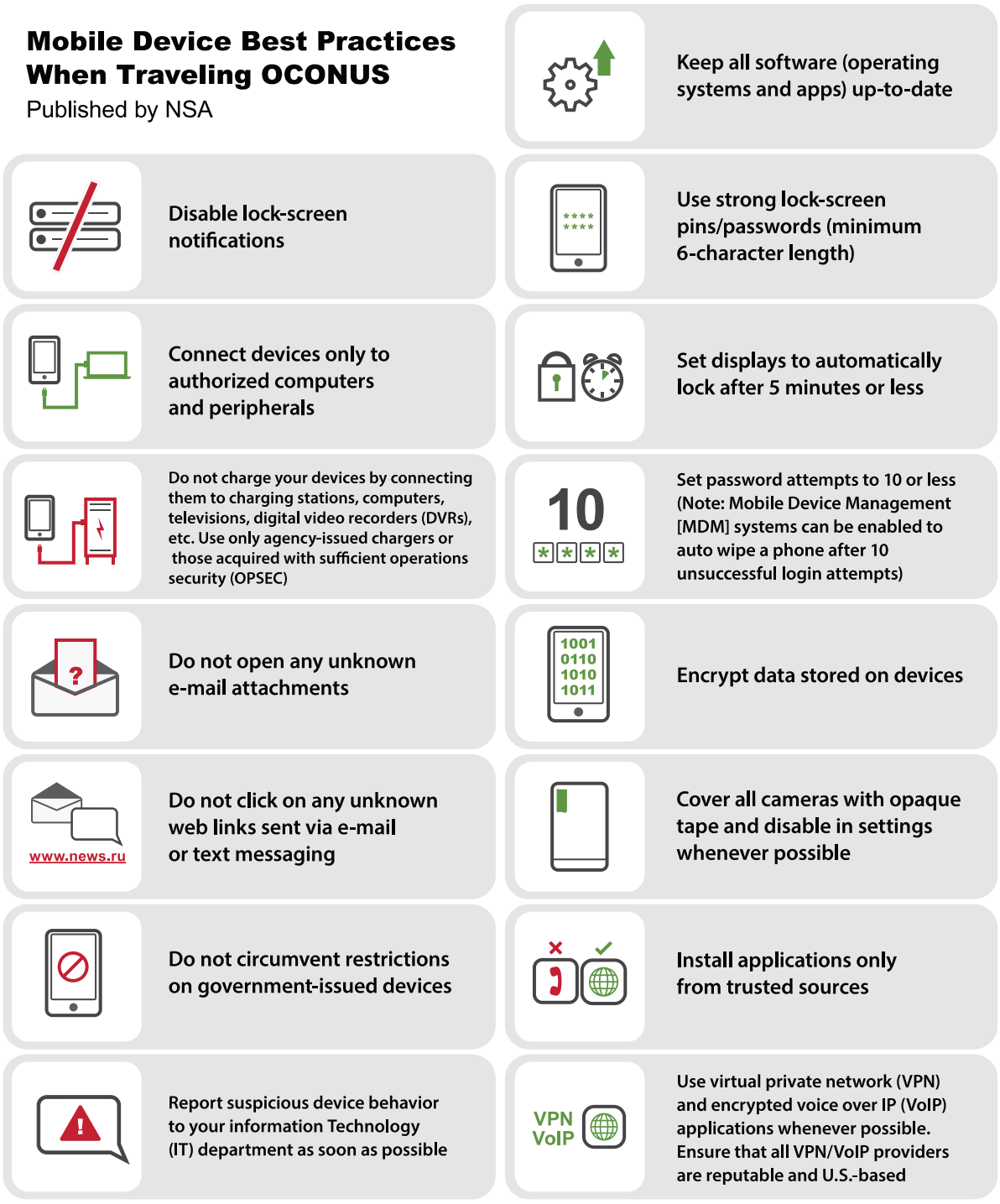



Figure 1. General Risk Mitigations When Traveling OCONUS

# Table of Contents

# Table of Figures



# Table of Tables

This page intentionally left blank

# 1 Introduction

Mobile devices such as smartphones and tablets facilitate work during foreign travel, including remote connections to enterprise networks and databases. Because of their portability and always-on state, mobile devices are susceptible to compromise, theft, physical damage, and loss, regardless of user location. Use of mobile devices during foreign travel often intensifies this risk. Both government and personal information are at risk, including government and personal user account information, contacts, and application data. Moreover, government and industry employees are often targeted by foreign adversaries seeking the government's confidential data and intellectual property and, in some cases, government employees' personal data.

Use of mobile devices OCONUS presents additional security risk. If compromised, a device's camera, microphone, Global Positioning System (GPS), functions, and other sensors may be used to eavesdrop on the traveler. Once compromised, the mobile device may be used to steal information or attack enterprise IT systems.

While on foreign travel, users and custodians of Government-Furnished Equipment (GFE) including wireless and mobile devices must be aware and understand that they are subject to the laws of the visited country. Foreign embassies and consulates, whether located in the U.S. or another country, also are considered foreign territory. When on foreign travel, government personnel should be aware that their activities likely will be monitored. Mobile devices (e.g., laptops, tablets, and mobile phones) are particularly vulnerable to interception and inspection, including possible malware infection. Unencrypted email and messaging communications and nonsecure phone calls often are targeted for interception by foreign adversaries seeking to extract intelligence information and execute attacks.

Use of agency-provided GFE in foreign countries may require equipment licensing, encryption restrictions, or reconfiguration to operate properly. However, if not installed and configured adequately, these enhancements and updates could increase the risk of agency data exposure, breach, and theft.

This guidance contains best practices regarding configuration and use of GFE mobile devices to safeguard information, backend enterprise systems, and users while on international travel OCONUS and outside U.S. territories. This guidance outlines physical and cybersecurity threats to GFE, procedures for before, during, and upon completion of travel, and other considerations for GFE users on temporary international travel.

## 1.1 Scope and Applicability

The term "*mobile device*" refers to *smartphones and tablets running mobile operating systems*, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations: *A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source.* Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

Travel to and use of GFE within countries listed on your agency's sensitive country list (SCL) requires additional security precautions, controls, and approval to protect the confidentiality and integrity of GFE-held data. SCL countries may be designated as sensitive based on reasons of national security, nuclear proliferation, regional instability, threat to national economic security, or terrorism concerns. Department/agency security officers will have access to a variety of information to provide travelers the most appropriate location-based threat informed guidance at the time of travel. U.S. Government (USG) employees traveling abroad for official business should consult the department/agency's security office about the security environment for the destination location. For USG employees travelling abroad for personal travel, it is recommended to adhere to your department/agency's security office location-based guidance and cautions as well as www.travel.state.gov for the latest information for the destination location.

This guidance is for international travelers carrying GFE on international travel, with the following limitations:

- It does not apply to classified systems and devices.
- The guidance pertains to use of GFE mobile devices to access Controlled Unclassified Information (CUI) and For Official Use Only (FOUO) information, which may include Personally Identifiable Information (PII), Sensitive Information, and Sensitive PII**.**
- Is applicable to all agency employees, contractors, detailees, and other personnel who use GFE to conduct business on behalf of the government.
- It does not apply to agency personnel who travel continuously or are stationed permanently overseas as part of their government duties, such as staff permanently stationed overseas or those who frequently cross U.S borders as part of their daily mission (i.e., Border Patrol agents).

While the scope of this document is GFE, the threats outlined are also applicable to personal devices used for official government duties through Bring Your Own Device (BYOD) or similar agency arrangements. If a traveler is tracked or eavesdropped, it does not matter what device is used. As such, users should consider protective countermeasures similar to those described herein when traveling with personal devices and conducting government duties on those devices.

## 1.2 Document Structure

The remainder of the document is structured as follows:

- Section 2 provides an overview of roles and responsibilities regarding use of mobile devices during international travel.
- Section 3 informs readers of physical and cybersecurity threats applicable to international travel as background for the best practices discussed in Section 4.
- Section 4 discusses best practices to mitigate threats discussed in Section 3, organized by procedures for before, during, and upon return from international travel.
- Section 5 summarizes the best practices for each phase of travel.
- Appendix A includes a set of checklists agencies can use for best practices and/or when developing their agency-specific policy.

# 2 Roles and Responsibilities

This section captures high-level agency programmatic and approval responsibilities for international travel with mobile devices. The responsibilities include the role(s) typically associated with carrying out those responsibilities, which may differ by agency. Among these responsibilities are:

- Agencies establish a process and issue guidance for distribution and operation of agency-issued mobile devices while traveling internationally that includes:
  - Identifying points of contact (POC) for approval and forms needed to request a mobile device and necessary apps.
  - Selecting devices and Enterprise Mobility Management (EMM) products.
  - Maintaining an inventory of devices and POCs for obtaining the device (or identification of responsible enterprise party for the devices).
  - Defining responsibilities for configuring the device prior to travel, monitoring it during travel, and inspection/sanitization of the device on return.
- The agency Security Office conducts threat assessments and maintains country-specific information on conditions and threats in the agency's SCL, including country-specific prohibitions against use of electronic devices and/or encryption technology. This information is used in foreign travel briefings for employees.
- The System Owner (SO) is responsible for developing and enforcing rules of behavior for mobile devices used to access information resources for systems under their authority.
- The Authorizing Official (AO) is responsible for approving use of mobile devices to access system resources as part of the system assessment and authorization process.
- The Chief Information Officer (CIO) or delegate is responsible for approving use of agency-approved mobile devices based on available resources and an employee's job function during the planned international travel. The CIO may delegate approval authority as needed.
- The Chief Information Security Officer (CISO) is responsible for approving any secure voice/messaging applications and requirements for preparation for, and use during, international travel. The CISO (or delegate) is also responsible for defining settings and configuration for the foreign travel profile for mobile devices and works with the agency Security Office to define requirements for post-travel evaluation and sanitization.
- The agency Security Operations Center (SOC) serves as the point of contact for travelers to report suspected security incidents.
- The device provisioning office/EMM administrator responsible for device provisioning, management, and reporting is responsible for configuring the device with the foreign travel profile, logging its use, and providing the device to the traveler.
- The device provisioning office/EMM administrator or Foreign Travel Forensics team is responsible for capturing the device baseline prior to travel, inspection of the device post travel, and sanitization of the device if necessary.
- Employees are responsible for:
  - Obtaining approval to travel with GFE and/or requesting issuance of a loaner device, with due consideration to the agency's approval processing timeline.
  - Reporting foreign travel to the agency Security Office per the requirements of their security clearance level.
  - Attending a foreign travel briefing, which includes security awareness training and guidance on use of mobile devices overseas.
  - Adhering to rules of behavior regarding use of GFE while on international travel.

# 3 Physical and Cybersecurity Threats

This section discusses potential physical and cybersecurity threats and risks associated with international travel as background for readers; it informs the best practices and mitigations described in Section 4.

## 3.1 Foreign Environment Threats

As representatives of the U.S. government, international travelers should expect to be targeted for surveillance and/or location tracking. Eavesdropping/bugging is a concern in many countries, particularly in hotel rooms. The likelihood of being tracked or having their mobile device attacked overseas varies based on the country visited, who the employee is or their position within the agency, and how interested state and nonstate actors are in the agency and/or the employee's work. Actions can be taken by the security services of the destination country or the security services of other foreign countries with a presence in the destination country. Employees on international travel should assume that their communications and activities are being monitored and therefore should conduct themselves accordingly. Agency employees traveling on a tourist passport or visa who conduct any official business while on travel should take any/all precautions as though they are traveling on official business.

## 3.2 Mobile Network Threats

Mobile devices can potentially connect to any available network, including untrusted wireless networks (i.e., Wi-Fi, Bluetooth, radio frequency [RF], Near-Field Communication [NFC], etc.) or foreign-owned/-operated cellular networks. This always-on connectivity presents heightened risk to agency mobile device users and device-stored data when the devices are used overseas. Wireless communications provide limited security from interception, jamming, or other threats.

Eavesdropping on wireless communications such as Wi-Fi, cellular and Bluetooth with commercially available equipment is common. Any Wi-Fi network (located within the continental U.S. [CONUS] or OCONUS)—whether free or paid—that is outside the control of the U.S. government should be considered untrusted and subject to monitoring. Techniques such as eavesdropping attacks can enable interception of data traffic to and from mobile devices, particularly when using untrusted Wi-Fi or cellular networks. Another threat is the use of International Mobile Subscriber Identity (IMSI) catchers (StingRay-type devices) that simulate cell towers and are used by adversaries to intercept and track mobile devices.

International mobile (cellular) networks may be owned or controlled by the host government, which can monitor all communications to and from the device. Foreign carriers may share infrastructure, which means that current Fourth Generation (4G) mobile systems and network protocols need to work with legacy Second Generation/Third Generation (2G/3G) systems and protocols. Legacy signaling protocols (e.g., Signaling System 7 [SS7]) are still widely used in the core networks of overseas mobile operators. SS7 has a flat trust model (all operators are trusted) and this trust level can and has been exploited to track users, intercept or block Short Message Service (SMS) text messages, redirect or eavesdrop on voice conversations, and drain a device user's bank account(s). Signaling traffic or user data may be routed in unexpected ways such as across borders as part of normal or failure mode operations in a core network.

## 3.3 Location Tracking

Geolocation and timing services are essential to the operation of any cellular network's operations and are widely used in mobile applications to provide context-specific information. These location services can be used for unauthorized geolocation of the user and the mobile device during travel, potentially threatening user safety, security, and privacy. Geolocation services can be provided to mobile applications through the device's Wi-Fi and cellular signals. Mobile applications may send geolocation data intentionally or unintentionally, maliciously or benign, or in unsecure ways making it an easy target for collection.

## 3.4 Malware and Surveillance-ware

There is an active surveillance industry that sells products and services to state and nonstate actors to deliver malware and enable tracking and monitoring of users through their mobile devices. Phishing techniques (email or SMS) can be employed by criminals or nation-state actors/foreign intelligence services to target high-value travelers (e.g., senior agency officials/executives). These services can install malware to compromise the device or attack agency backend systems or to install surveillance-ware, which can intercept calls and text messages or activate the mobile device's camera or microphone without the user's knowledge. Physical access to the mobile device—e.g., if the user is required to surrender the device during a border crossing or if the device is left unattended in a hotel room or other location—is a direct vector for delivery of such malware to the device.

In addition, some corporations gather marketing information from mobile devices (e.g., through adware included in mobile apps). Some nation-state and transnational criminal organizations can purchase this data from commercial firms, exposing information on device and app usage as well as personal information associated with apps.

Spyware companies have developed 'zero-click' attacks that deliver and execute the malware simply by sending a message to the target's phone. The Pegasus spyware/surveillance-ware, first identified in 2016,[1] has been in the news recently with discovery of its use to track journalists, executives, and human rights activists.[2] This particular cyberespionage tool is designed to evade mobile operating system defenses and leave few traces. It is a relatively expensive and very targeted malware tool; governments that use this surveillance-ware are interested in particular targets, considered high value by the adversary.

Carriers controlled by foreign governments can push malware directly to the mobile device. This action may be accomplished by the carrier requesting that the device firmware or operating system be updated. The user may or may not have to acknowledge this change for it to successfully update their mobile device.

## 3.5 Border Crossings

Foreign and domestic government officials at international border crossings can—and sometimes do—ask travelers for access to their smartphones, tablets, and other mobile devices. They may also request that the traveler unlock the device and/or provide access passwords. Complying with the

[1] The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender - The Citizen Lab

[2] Private spy software sold by NSO Group found on cellphones worldwide - Washington Post

request can allow the agents to search, read, or copy data on the device such as documents, emails, passwords, contacts, browser history, social media account information, and Subscriber Identity Module (SIM) card information.

Minimizing the sensitive agency or personal data stored on the device reduces the amount of data that could be exposed or otherwise compromised should the mobile device be accessed by unauthorized persons.

Government employees should understand the destination country's laws regarding border searches. If the traveler refuses to comply with the request to unlock the device, border officials may seize the device or detain the employee until they agree to surrender it. Employees should power off their mobile device prior to crossing the border. If the mobile device is removed from the employee's view for any length of time and then returned, the employee should immediately power down the device and as soon as possible report the incident to their immediate supervisor, who should follow incident-reporting procedures. Likewise, if the device is seized and not returned, the employee immediately should report the incident to their immediate supervisor and to the local U.S. embassy or consulate.

## 3.6 General Crime

Mobile devices are expensive and are often targeted for theft. Travelers should maintain close awareness of all devices they are carrying and how a thief could access them (incidents such as bags being surreptitiously cut open while travelers are carrying them are not uncommon). Stolen devices may be sold on the black market for cash or to the security service of a local country or another foreign country. The best prevention is to not use electronic devices in public, thereby reducing the likelihood of being targeted.

## 3.7 Recognize the Signs of a Possible Attack

Travelers may be unsure or unable to identify compromises of their mobile devices. Unfortunately, many symptoms of compromise are confused with using foreign internet service providers to connect. Signs of compromise and malicious activity often include those depicted in Figure 2.


**Figure 2. Signs of a Possible Attack**

Malicious activity also may include adversaries downloading existing pictures, recording and uploading audio and video, and executing denial of service attacks.

# 4 Travel Procedures

This section provides recommended procedures to mitigate the threats described in Section 3. The best practice recommendations are organized by phase of travel: before, during, and upon completion of international travel, as summarized in Figure 3 below.

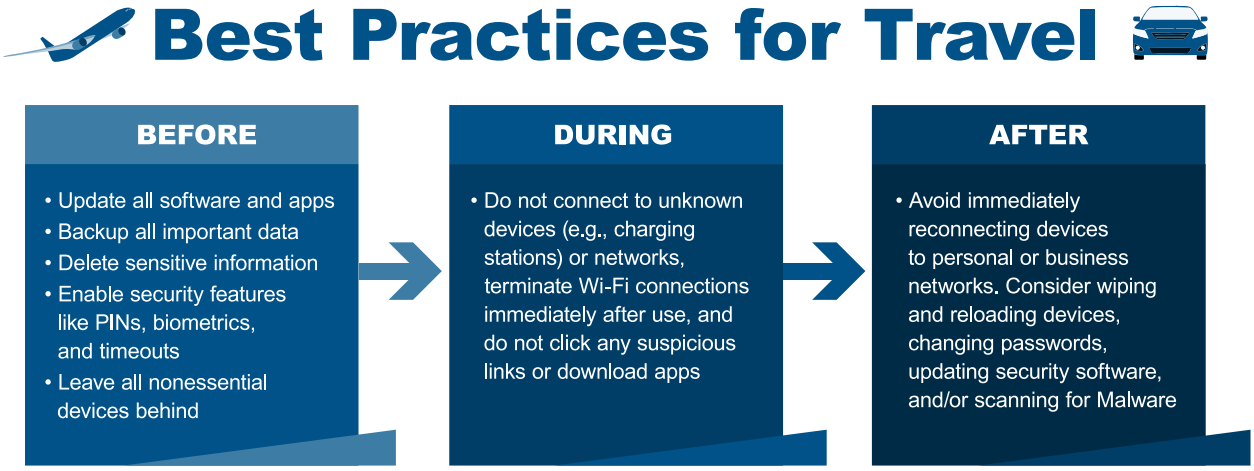



Figure 3. Best Practices for International Travel with Mobile GFE Devices[3]

## 4.1 Prior to Travel: Device Protection

**Pre-Travel Quick Tips**:[4]

- Prepare dedicated (e.g., loaner) devices with limited contacts and emails for the exclusive purpose of your imminent travel.
- Acquire and install new SIM cards for the destination service area. Using international SIM cards purchased domestically is preferable, however, if this option is not possible, make sure to use good operations security (OPSEC) by purchasing SIM cards from standalone stores, not from a store or kiosk at the airport.

Agency-issued loaner mobile devices should be configured with minimal features and voice/data applications based on mission need to help mitigate risks of foreign cyber or electronic surveillance.

The agency should establish a foreign travel e-mail distribution list that includes, e.g., the agency's Foreign Travel Forensics team, Security Office, and cybersecurity team (SOC).

Follow all agency mobile device security requirements for specially configured devices. Critical techniques to mitigate risks of mobile devices that remotely access agency systems and data from overseas include the following:

- Central management of the device and applications.
- Baseline secure configuration with unneeded features and capabilities disabled.
- Strong authentication of the user and the device.
- Agency guidance-compliant password to unlock the device.
- Minimum apps and data required for official business.

[3] Source: Overseas Security Advisory Council | www.OSAC.gov

[4] Mobile Device Best Practices When Traveling OCONUS. NSA. May 2018.

- Protection of data at rest and in transit.
- Monitoring the device for deviation from security guidance and for indicators of mobile threats.
- Physical security.

Secure Digital (SD) cards or other external media should not be used/issued with the device.

### 4.1.1 Manage Mobile Devices and Applications

Agency-issued loaner mobile devices should be managed and monitored by an agency EMM system. An EMM system allows the agency to centrally manage mobile devices and enforce security policies on the devices, including configuration change detection, user and device authentication requirements, remote data wipe, remote configuration, and asset/property management.[5] All mobile devices must be accounted for in a Federal Information Security Modernization Act (FISMA)-inventoried system.

If the traveler is issued a loaner GFE mobile device, the issuing office must ensure that the mobile device is running the most current mobile operating system (OS) as well as the current version and security patches for installed apps and firmware. While it may seem more cost efficient to use older smartphones as loaner devices, such devices may not support the latest mobile OS. In addition to patching vulnerabilities, new OS versions often include security architecture improvements that provide resilience against yet-undiscovered vulnerabilities or weaknesses. An up-to-date OS is the first line of defense against threats to a device.

### 4.1.2 Install Minimum Set of Managed Mobile Applications

Agency mobile applications configured on a loaner mobile device should be managed by the agency. To reduce risk of exposure of agency or employee personal data during travel, only the minimum set of mobile apps and data required by the traveling employee to conduct official business (e.g., secure email, secure browser, office productivity) should be installed on the device, as determined by the agency's Foreign Travel Policy. The devices should be configured to disallow user download and installation of apps from unofficial app markets or unknown sources. The agency can use its EMM system to define a foreign travel profile with these configurations and settings and push that profile to the loaner mobile device.

To reduce the amount of email data stored on a device, the AO (or delegate) may consider limiting mailbox size and access to enterprise email archives and issuing the employee a separate, temporary internal email account for the loaner device. Use of virtual mobile infrastructure/virtual desktop infrastructure to minimize the data and applications on the device may also be considered.

### 4.1.3 Install Mobile Threat Defense Software

Mobile devices provide ready access to remote email, files and other government data while on travel, but they present security challenges for users and government agencies as well as opportunities for malicious foreign interests. Theft and data breaches are a major concern. If successful, malicious foreign actors could gain access to sensitive agency data.

[5] Refer to your agency's approved product list or the General Services Administration (GSA) website for information on EMMs.

Information security mechanisms for agency enterprise IT systems and services should be used to protect mobile devices. For example, email should be scanned by the agency email servers before it is delivered to the mobile device. An EMM system checks device configuration and compliance with device security guidance when the employee connects to email or other agency resources. However, these security checks may occur infrequently during travel.

As an additional countermeasure to detect anomalous behavior in real-time, mobile threat defense (MTD) should be installed on the device. This software monitors device, application, and network behavior. It can detect suspicious and potentially malicious application or network activity and notify the EMM administrator and the device user. The software should be configured to remediate malicious behavior, either independently or via integration with the EMM system. The information collected by MTD software should be limited to the minimum data necessary to perform its function.

Approval of MTD software for real-time security monitoring of the mobile device should be coordinated with the agency's CISO or appropriate agency-designated authority and is the overall responsibility of the AO.

### 4.1.4 Enforce Authentication Requirements

The device should be configured to ensure that authentication and access controls are required to access the device and the data on the device. Device unlock should be configured to require a strong password known only by the user and if the device is powered off, the password should be required when it is powered on. Use of biometrics makes it more convenient to use stronger device lock passwords because the password does not need to be entered all the time. If agency policy allows use of biometric characteristics to unlock the device, travelers should be aware that government officials can compel users to unlock a device with their fingerprint or a face scan.

Email and other allowed agency mobile apps on a device should require user authentication, either by using the device screen unlock authentication or a separate authentication method. Access to the agency's enterprise resources should require mutual identification and authentication of the user and the device to the resource and of the resource to the device. Users should be instructed to choose passwords for use on their agency-issued mobile device while on international travel that are different from those used with their standard GFE.

### 4.1.5 Protect Data At-Rest and In Motion

All data on mobile devices should be encrypted using Federal Information Processing Standard (FIPS) 140-2 or 140-3 validated encryption schemes. Passwords to encrypt the data should comply with agency requirements. Implementing additional countermeasures such as file and data encryption or digital rights management can further protect the confidentiality of information residing on the device.

The device's "Find My Device" and remote wipe features should be enabled so the EMM can perform remote wipe to protect data from unauthorized access in the event of device loss, theft, or suspected compromise.

### 4.1.6 Secure the Wireless Communications Link

The wireless interface—the link between a mobile device and a network endpoint or between two mobile devices—is vulnerable to attacks. Cellular infrastructure may not be owned by the carrier,

may be controlled by a foreign government, or may be accessible to other carriers and to maintenance subcontractors. The risk of interception of cellular and Wi-Fi communications during international travel is high.

All network access to enterprise data, whether through mobile apps or web browsers, should use Hypertext Transfer Protocol Secure (HTTPS) or other appropriately encrypted network protocols with mutual authentication of both the requesting app or browser and the enterprise system. Mobile app vetting tools can help detect use of insecure network protocols by apps. A Virtual Private Network (VPN) may also be appropriate to provide an additional layer of protection (e.g., in case of vulnerabilities in the HTTPS implementation).

For devices issued to senior agency officials/executives and authorized personnel, an additional layer of separation between the mobile device and foreign Wi-Fi or cellular networks may be considered, such as use of a portable wireless access point ("hotspot"). The hotspot device should be secured in accordance with Wi-Fi guidance.

### 4.1.7 Disable Nonessential Mobile Device Capabilities

Mobile device capabilities, features, and ports that may be allowed for use in the U.S. but are not required during international travel, could be exploited. To reduce risk, the following capabilities on the device should be disabled: infrared, Bluetooth, Near-Field Communication (NFC), and other unneeded tools and applications such as those pre-installed by the mobile device vendor or the mobile cellular carrier.

Settings to automatically join new Wi-Fi networks should be disabled. Location services should be disabled for mobile apps that are not mission essential.

### 4.1.8 Protect Voice and Text Communications

Voice and text message services are not secure and should not be used for CUI communications unless authorized point-to-point encryption is used. Exceptions may be granted if approved secure voice and/or messaging applications are installed on the device. Approval of such applications should be coordinated with the agency's CISO or appropriate agency-designated authority.

### 4.1.9 Capture Device Baseline Configuration

Following provisioning and configuration of the mobile device, and prior to issuance of the device to the traveler, the device administrator should use a mobile device integrity validation tool to capture the pre-travel baseline configuration of the GFE mobile device or loaner mobile device. Such tools provide the means to detect firmware and/or hardware modifications to a mobile device between two points in time. Upon return, the device should be examined so the post-travel configuration can be compared against the pre-travel baseline configuration to detect any malware insertions or unauthorized modifications of the device's settings, configuration, software, firmware, and hardware.

## 4.2 During Travel: Device Protection

**During-Travel Quick Tips:**[6]

- Always maintain positive physical control of devices (do not leave your agency-issued devices in a hotel safe).
- Turn off unused wireless communications (e.g., Bluetooth, NFC, Wi-Fi).
- Disable GPS and location services (unless their use is required).
- Do not connect to open Wi-Fi networks.
- Do not connect personal devices to official devices or vice versa.
- Regularly inspect devices for signs of tampering.
- Avoid logging into USG networks unless necessary and use a VPN to connect to government networks.

Figure 4 summarizes some best practices for international travelers. Government travelers should be especially vigilant and wary to mitigate loss and theft of their device; eavesdropping of their conversations, screen activity, and data; and other threats to the confidentiality, integrity, and availability of information stored or accessed on their mobile device for the duration of their travel. Traveling government employees are responsible for complying with the agency's mobile device rules of behavior and exercising continuous security and safety awareness while on travel.

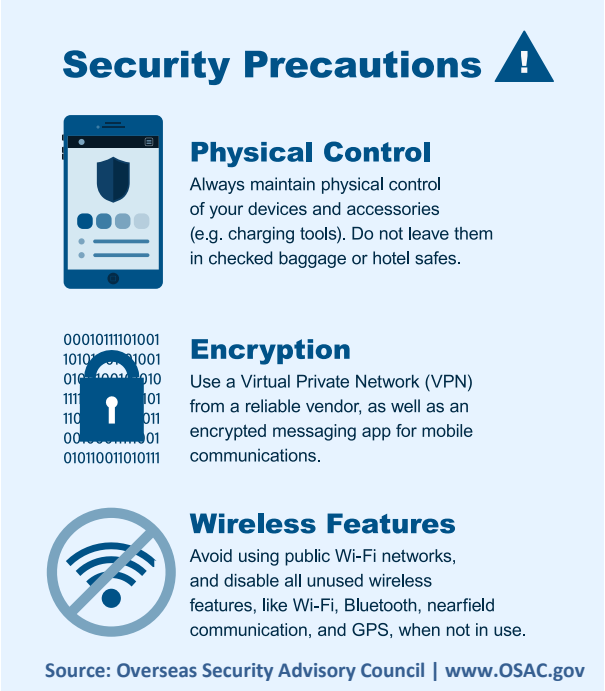



**Figure 4. Security Precautions for International Travelers**

### 4.2.1 Always Maintain Possession of Device

Government employees should always maintain physical possession of their agency-issued mobile device during international travel. This advice means a government employee should never leave their device unattended in a vehicle, hotel room, hotel safe, conference room, work area, or other location. Devices should be turned off when not in use. Powering down devices reduces battery drain, location tracking, and potential of brute force password attacks. The mobile device should be transported in carry-on luggage, rather than in checked baggage, and users should maintain awareness of the device when going through airport or building access X-ray machines and other physical security examination equipment.

Government employees should not hand over control of an agency-issued device, unless specifically required to do so, such as at a border crossing (see section 4.2.3 for guidance on travel to secure foreign facilities). Before handing over control of GFE, for example to a border agent or depositing it in a temporary storage location, government employees should turn the device off and remove and keep the battery (if physically possible) as well as the device's Universal Integrated Circuit Card (UICC) or SIM card. Understanding the risk of losing physical control of the device, as soon

[6] Mobile Device Best Practices When Traveling OCONUS. NSA. May 2018.

as the GFE is returned, users should inspect it for any obvious signs of tampering before replacing the battery and UICC or SIM card and powering it on. Travelers also should be made aware of the threat and frequency of theft of expensive mobile devices in foreign countries. Devices should not be used in public where they may be observed and targeted. Device theft could be cover for hostile action by the security services of the destination country or those of a foreign country with a presence in the destination country.

### 4.2.2 Foreign Travel Through Customs and Ports of Entry

Government travelers are subject to the destination nation's laws, including those defining local security requirements and protocols when entering or traveling within the destination country or through its ports of entry. These requirements or protocols also include any inspections or requests for inspection of agency GFE made by the destination country's border security or law enforcement officials. Ports of entry include airports, seaports, train stations, and roadway border crossings.

When going through a checkpoint, devices should be turned off and authentication credentials (Common Access Cards [CAC], Personal Identity Verification [PIV] cards, hardware tokens, etc.) should be stored separately from the device.

Travelers going through ports of entry, including the U.S., may be required to turn on or unlock their GFE devices as part of port of entry and Customs inspections. Agency employees should adhere to local port of entry and Customs security requirements and protocols and comply as directed. Not doing so may result in a device being confiscated and/or the traveler being detained until they comply.

### 4.2.3 Procedures for Foreign Travel to Secure Foreign Facilities

Travelers are subject to destination nation laws, including local security requirements and protocols when visiting secure foreign facilities and sites such as government offices, laboratories, or other locations. Agency employees visiting secure foreign facilities should adhere to local security laws, requirements and protocols and secure their devices as instructed.

GFE devices stored outside a secure facility or within a designated storage location should be powered off, encrypted and otherwise sufficiently hardened, and authentication credentials should either be kept on their person or stored separately or in a lockbox for which the user maintains possession of the key to prevent access to or compromise of the device.

### 4.2.4 Signs of Tampering

Regularly inspect devices for signs of tampering. Tampering may appear as:

- New nicks or scratches, especially near electronic connections.
- Dents in the case along seams or glass screens.
- Residue left from tape or other adhesives.
- Significantly reduced battery levels when compared to those last observed on the device.
- Change in power state (i.e., the device is turned on when it is returned, but it was turned off when you handed it over or vice versa).
- Changes in how the power or other cables are wrapped or stored.

Any sign of tampering should be reported to your supervisor or other appropriate POC.

### 4.2.5 Turn off Wireless Communications

Unless mission essential, turn off Bluetooth and ensure it remains disabled. If Bluetooth is allowed, follow your agency guidance. If Wi-Fi use is allowed, turn it off when it is not in use. When these services are turned on the radios are constantly searching for Wi-Fi networks to which to connect. This constant pinging can be used to locate the device user. Turning off Wi-Fi will help conserve battery life. Government travelers also should disable NFC communications because these connections may be monitored by payment apps or hotel apps for various "tap" behaviors and provide a conduit for attacks.

### 4.2.6 Be Careful When Using Untrusted Wi-Fi Networks

Do not connect to open Wi-Fi networks and avoid connecting to secured Wi-Fi networks at hotels (regardless of size or country of ownership), restaurants, airports, or networks of other commercial or public institutions other than the U.S. Government. If it is necessary to use one of these networks, be sure that all security measures are in place, to include VPN and mobile device security. Confirm the name of the Wi-Fi network (the Service Set Identifier [SSID]) before connecting, such as the name of a Wi-Fi network shown on a permanent public sign in an airport. When connecting to Wi-Fi networks, a login or other splash page may appear in your browser. Be aware that these pages are the perfect place for targeting travelers who may be complacent from clicking through pages in hotels and cafés domestically and may not be surprised if they are asked to submit personal information and click a button, etc. Pages requiring a passcode are no more secure than others.

Wi-Fi networks, once joined, are then saved to the device by default. If a Wi-Fi network is used while traveling, it and any public Wi-Fi network should be removed from the list of previously joined networks. Travelers should manually remove all joined Wi-Fi networks after use by navigating to "Settings" on their device.

### 4.2.7 Be Wary of Text Messages and Update Requests

Among the common attacks used against high-profile travelers are SMS messages that contain links to web pages with malware that compromises the mobile device. These attack messages may imitate the standard "welcome" text message arriving visitors get from the local mobile network operator informing them of local mobile and data rates or notifications to install apps to access a local cellular or Wi-Fi network. The messages are effective because mobile device users are familiar with them and may expect them when they travel to a new service location. Government employees should recognize these attempts and never click on such links, nor should they install any certificates (enterprise or otherwise), apps, or log in to any systems that these links present.

Other attacks that may be less obvious are firmware, OS, or app update notifications that arrive as the traveler enters the country (e.g., notification to install a COVID-19 tracking app). Users may be accustomed to accepting these updates and need to be aware that the "updates" may be a method to compromise the mobile device and monitor user communications and activities. Since the device was configured and updated to the most recent OS versions and apps prior to delivery to the employee, there should be no need to update the device during travel. However, if an emergency patch or update is necessary, notification should come via your agency EMM.

### 4.2.8 Verify Location Services Settings

Apps frequently collect location and personal information to enhance user experience or sell services. However, this information can reveal the device's location and can be used to track the employee's activities. Ensure that location tracking is turned off for all installed apps, system settings, and any other services unless specifically directed by the AO or SO. Ensure all privacy settings are configured so apps and services cannot access data and location services as part of their normal function. Enable these features under the guidance of the AO or SO.

### 4.2.9 Separation of Personal and Agency Devices

Agency employees must not connect their personal devices and agency devices to include connecting a personally owned Bluetooth headset to an agency-provided mobile device or connecting an agency-provided mobile device to a personal laptop. Personal devices do not have the full cyber protections available to agency devices, creating a significant weak point if they are connected. In addition, do not accept or use "loaner" devices that can be used to connect to your agency-issued devices such as Bluetooth headsets that may be offered by airlines or hotels.

### 4.2.10 Report Security Incidents Immediately

Agency employees should immediately report incidents involving loss, theft, compromise or suspected compromise of their agency-issued mobile device during international travel per agency instructions. Employees also should report immediately suspected loss, compromise or unauthorized disclosure of CUI or PII during travel. Agency employees who are required to surrender the agency-issued device for inspection at customs or a border crossing should not disclose passwords used for encryption or access control. Agency employees who are coerced into revealing mobile device decryption or unlock passwords must immediately report the incident per agency instructions and change the passwords as soon as possible.

## 4.3 Post-Travel: Return and Inspection of Device

**Post-Travel Quick Tips:**[7]

- Physically inspect your travel devices.
- Wipe and reload your travel devices.

Upon completion of international travel, the employee should return the mobile device, any portable media (e.g., SD card), and device passcodes to the device-issuing office as soon as possible, i.e., upon return to the office. The device should not be connected to an agency network. The employee's mobile device should be scanned with a mobile device integrity validation tool to identify changes to the device's OS, applications, software, firmware, and hardware, and to determine the risk level of any discovered changes.

Per agency policy, and based upon risk level, the mobile device may be returned to the traveler or retained for further forensic analysis. The AO or SO is responsible for rendering a risk management decision on reset/reuse of the device based on the results of the digital media analysis and guidance. Data on a loaner device will be sanitized before it is reissued or retired. It is important to understand that a soft or hard reset will not permanently erase the data on a mobile device, nor will a file

[7] Mobile Device Best Practices When Traveling OCONUS. NSA. May 2018.

management utility permanently remove files. On completion of device examination and sanitization, the device will be disposed of appropriately. The loaner device inventory will be updated to reflect its unavailability and the international service plan for the disposed device will be discontinued per agency guidance.

### 4.3.1 GFE Return Procedures[8]

1. All GFE loaner devices used during foreign travel should be returned to the designated device issuing office within the timeframe specified when the device was issued (e.g., within two business days of the conclusion of foreign travel) for device integrity checking evaluation or similar capability and sanitization. Sanitization processes must meet the minimum "Clear" sanitization level and adhere to standards as defined in *NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, Appendix A*.
2. GFE loaner devices used during foreign travel may not enter agency-designated protected areas until the sanitization process is completed and approved for specific use in such areas.
3. GFE loaner devices (e.g., mobile devices, Universal Serial Bus [USB], and tablets) accessing the agency network or agency information outside any approved VPN or secured remote access channels cannot be connected to the agency network or systems until evaluation and sanitization has been performed by the agency's authorized organization.
4. No agency data may be transferred to or from GFE loaner devices (e.g., downloading or sharing information through mobile devices, USB, and tablets) accessing the agency network or agency information outside any approved VPN or secured remote access channels until evaluation and sanitization has been performed by the agency's authorized organization.
5. For permanently issued GFE, refer to the device provisioning entity for agency network or system connectivity, data transfer, and evaluation and sanitization requirements.
6. Additional measures may be required for GFE utilized when travelling to agency SCL-designated countries. Refer to the device provisioning entity for specific requirements for loaner or permanently issued GFE used during foreign travel to SCL-designated countries.

## 4.4 Other Considerations

### 4.4.1 High Value Personnel/Access to High Value Assets

Additional considerations should be given to devices that may contain sensitive data or communications and devices which may be used to access a system designated by an agency as a High Value Asset (HVA). Even if travel only consists of general risk locations, the agency's risk level rises as the value of data at risk increases. Security measures should include those listed in Figure 1. General Risk Mitigations When Traveling OCONUS in the Executive Summary. Additional measures to limit exposure of sensitive information and targeting can include, but are not limited to:

- Employment of MTD software and monitoring while on travel.
- Additional restrictions pushed to the device by the EMM.
- Additional end-user training on threats and remediations pertaining to the country of travel.
- Setting up a separate proxy account for travel to a country on the agency's SCL:

[8] Appendix A.2 contains a post-travel checklist.

- This account should have the minimum information needed for the travel transferred from the user's primary account.
- Email should be selectively or fully forwarded from the existing account to the proxy account.
- Information created/received while on travel should be reviewed for potential malware and indications of compromise upon return and before transferring to the user's primary account.
- The proxy account should be flagged in enterprise monitoring systems for access attempts after travel is completed.

- Issuance of a mobile hotspot/VPN.
- Use of a loaner or burner device.

**Scenarios for this level of consideration may be:**

- Executive level travel. High-profile U.S. Government personnel are top targets for foreign security services. If a mobile device is required while they are traveling overseas, they should carry or employ a travel commercial mobile device rather than their Government-furnished mobile device.
- Travel to country on the agency's SCL
- Federal agents participating in any operation where OPSEC is a priority.

### 4.4.2 Multiple Travel Destinations

Additional considerations should be given to travelers with multiple countries on the itinerary, including layovers. Risks to federal employees change and evolve based on their location of travel. Agencies monitor travel threats in different countries and evolving cyber campaigns within them. Agencies should ensure employees are briefed of known threats along with the appropriate mobile security mitigations.

# 5 Summary: Overseas Travel Best Practices

When traveling with a GFE mobile device, it is important to know that travelers can decrease their vulnerability by recognizing common attack vectors and signs of asset compromise. Malicious activities may include adversaries downloading existing pictures, recording and uploading audio and video, and executing denial of service attacks. Risks of IT asset compromise also can be mitigated using the best practices discussed in this document and summarized in the figure below.

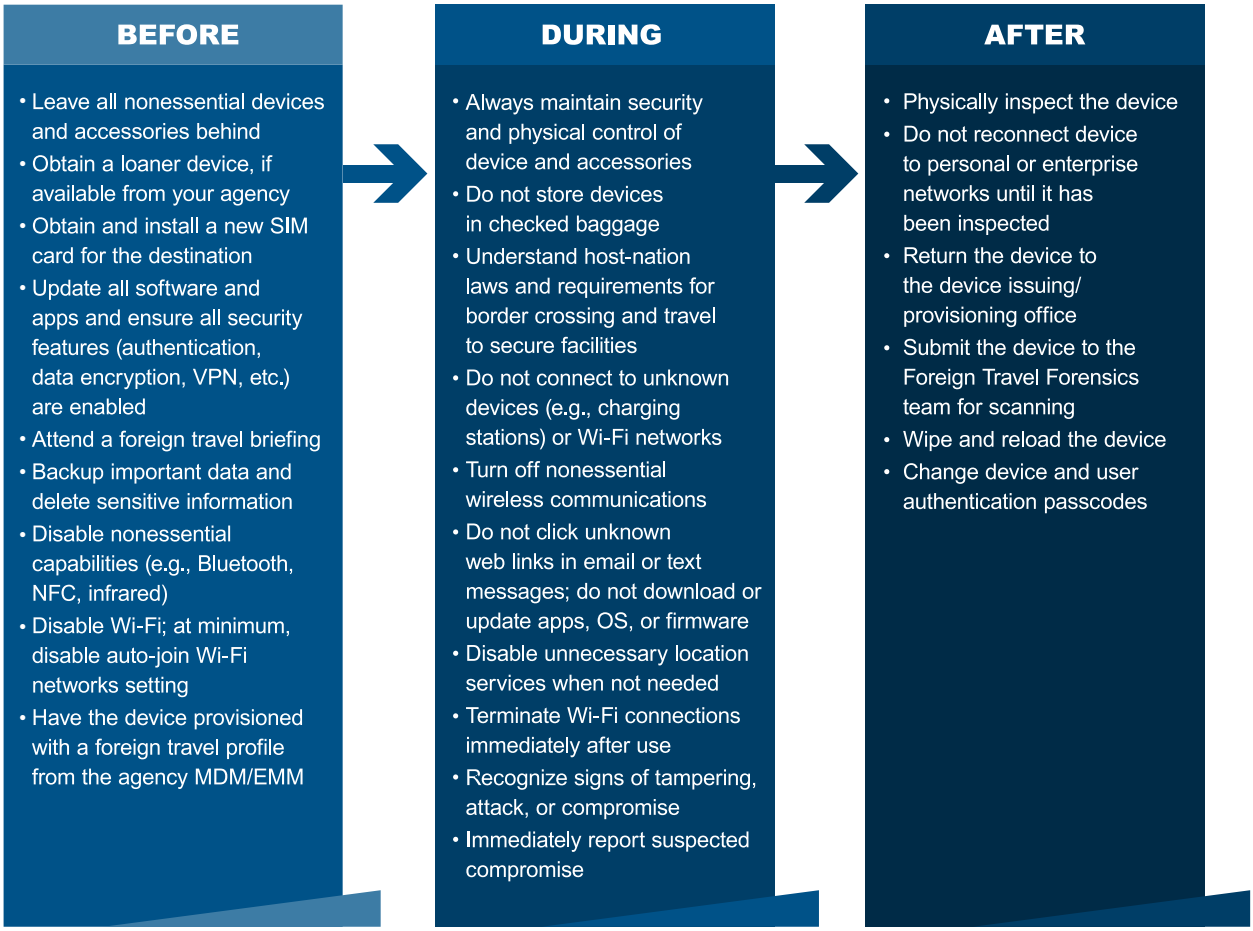



Figure 5. Best Practices for International Travel

# Appendix A Travel Checklists

The following checklists should be used by agency personnel to ensure all pre- and post-trip activities are completed. Each checklist identifies the key activities for general and high-risk countries, with callouts for platform-specific activities as needed.

## A.1 Pre-Travel Checklists

Table 1. IT Asset Foreign Travel Pre-Travel Process: General Risk Countries

| Process Descriptions | Status |
|---|---|
| **For All IT Assets** | |
| Foreign Travel Waiver request submitted to agency security office for approval. | |
| Agency security office identifies Country/Region encryption Laws. | |
| Agency security office identifies country risk level and approves or denies Foreign Travel Request. | |
| Approved Foreign Travel Waiver request sent to pre-/post-travel forensics team at least 48 hours prior to travel. | |
| Foreign Travel User Awareness Briefing provided to the device user. | |
| General Risk Foreign Travel Baseline applied to the device through MDM and validated. | |
| External Storage Encryption (SD Card, etc.) verified. If not necessary for travel, all removable cards must be removed. | |
| Unnecessary agency data stored on the device has been removed or minimized prior to travel. | |
| Take a pre-travel configuration baseline snapshot (using a mobile device integrity validation capability). | |
| Provide user an agency MiFi Device and configure their IT asset to use the MiFi. | |
| Agency IT asset charger(s) provided. | |
| Perform a Backup of all data. | |

595

Table 2. IT Asset Foreign Travel Pre-Travel Process-High Risk Countries

| Process Descriptions | Status |
|---|---|
| **For All IT Assets** | |
| Foreign Travel Waiver request submitted to agency Security Office for approval. | |
| Agency Security Office identifies Country/Region encryption Laws. | |
| Country identified as high-risk; Foreign Travel Waiver request submitted by agency Security Office to pre-travel forensic team at least one week (five business days) prior to travel. | |
| Foreign Travel Approval received from agency CISO/international travel forensic team. | |
| Foreign Travel User Awareness Briefing provided to the device user. | |
| Unnecessary agency data stored on the device removed or minimized prior to travel. | |
| An advanced monitoring or secure container solution is installed. | |
| VPN software installed and user access validated as functioning. | |
| High-Risk Foreign Travel Baseline applied to the mobile device. | |
| Create backup of all data. | |
| Remove External Storage/SD Card. | |
| User provided an agency MiFi Device, and their IT asset is configured to use the MiFi. | |
| Agency IT asset charger or power cable provided. | |
| **Additional Steps for Mobile Devices** | |
| High-Risk Foreign Travel Baseline is applied to the mobile device through an EMM system and validated. | |
| Remove two-factor authentication tokens from device. | |

## A.2 Post-Travel Checklist

Following is the checklist for assets returning from travel to general-risk countries. There is no checklist for assets returning from high-risk countries since those assets are to remain in the high-risk pool and handled per agency policy.

Table 3. IT Asset Foreign Travel Post-Travel Process

| Process Descriptions | Status |
|---|---|
| **For All IT Assets** | |
| Immediately upon return from travel perform a post-travel analysis to determine compromised state. | |
| Remove advanced monitoring or secure container, if returning from a high-risk country. | |
| Remove Foreign Travel Baseline and reapply domestic baseline. | |
| Restock agency MiFi device. | |
| Return external storage/SD Card. | |
| Restore data from previously created backup. | |
| **Additional Steps for Mobile Devices** | |
| Reinstall two-factor authentication tokens, where necessary. | |

# References


1. "Mobile Device Best Practices When Traveling OCONUS," NSA Central Security Service. June 7, 2018. Available: Mobile Device Best Practices When Traveling OCONUS (nsa.gov)

2. NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST. September 2020. Available: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)

3. DHS Sensitive Systems Handbook (4300A) "International Travel with Mobile Devices," Version 1.7. DHS. April 2, 2018.

4. "General Risk Foreign Travel Plan," Department of Justice. June 2020.

5. Enterprise Mobility Management. U.S. GSA. https://www.gsa.gov/technology/technology-purchasing-programs/telecommunications-and-network-services/enterprise-mobility/enterprise-mobility-management

# List of Acronyms

| Acronym | Definition |
|---|---|
| **2G** | Second Generation |
| **3G** | Third Generation |
| **4G** | Fourth Generation |
| **AO** | Authorizing Official |
| **BYOD** | Bring Your Own Device |
| **CAC** | Common Access Card |
| **CIO** | Chief Information Officer |
| **CISO** | Chief Information Security Officer |
| **CUI** | Controlled Unclassified Information |
| **DHS** | Department of Homeland Security |
| **DoD** | Department of Defense |
| **DVR** | Digital Video Recorder |
| **EMM** | Enterprise Mobility Management |
| **FIPS** | Federal Information Processing Standard |
| **FISMA** | Federal Information Security Modernization Act |
| **FOUO** | For Official Use Only |
| **GFE** | Government-Furnished Equipment |
| **GPS** | Global Positioning System |
| **GSA** | General Services Administration |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **HVA** | High Value Asset |
| **IT** | Information Technology |
| **MTD** | Mobile Threat Defense |
| **NFC** | Near-Field Communication |
| **NIST** | National Institute of Standards and Technology |

| Acronym | Definition |
|---|---|
| **NSA** | National Security Agency |
| **OCONUS** | Outside the Continental U.S. |
| **OPSEC** | Operations Security |
| **OS** | Operating System |
| **PII** | Personally Identifiable Information |
| **PIV** | Personal Identity Verification |
| **POC** | Points of Contact |
| **RF** | Radio Frequency |
| **SCL** | Sensitive Country List |
| **SD** | Secure Digital |
| **SIM** | Subscriber Identity Module |
| **SO** | System Owner |
| **SOC** | Security Operations Center |
| **SS7** | Signaling System 7 |
| **SSID** | Service Set Identifier |
| **UICC** | Universal Integrated Circuit Card |
| **USB** | Universal Serial Bus |
| **USG** | U.S. Government |
| **VoIP** | Voice over IP |
| **VPN** | Virtual Private Network |