Homeland Security

DHS Policy Directive 4300A, Information Technology System Security Program, Sensitive Systems

Attachment Q

International Travel with Mobile Devices

Version 1.0

April 25, 2022

Protecting the Information that Secures the Homeland

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	April 25, 2022	Initial Draft updated processes and authorities - Jamila Moore, IT OPS

CONTENTS

1.0 INTRODUCTION

This document provides guidance and recommendations to support Department of Homeland Security (DHS) policy, *Security of DHS-Issued Devices During International Travel* (hereafter referred to as *International Travel* policy) of *DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems* (hereafter referred to as *DHS 4300A*). The *DHS 4300A* contains wireless security requirements that apply to all mobile devices and wireless systems; the *International Travel* policy contains additional specifications regarding configuration and use of mobile devices to safeguard information, systems, and users of mobile devices while on international travel outside the continental United States and its territories.

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 outside the U.S. presents additional security risk. Once compromised, a device's camera, microphone, Global Positioning System (GPS), functions, and other sensors may be used to eavesdrop on the traveler and the mobile device may be used to steal information or attack other DHS systems.

To reduce risk to DHS Information Technology (IT) assets and data, the International Travel policy under strict guidelines allows Authorizing Officials (AOs)[1] to make a risk-based decision on whether to allow DHS employees to take Government Furnished Equipment (GFE) on international travel. DHS employees must possess proper clearance/travel orders and a mission need to access DHS information via DHS GFE while in the United States or abroad. DHS GFE mobile device, referred to as DHS-issued mobile device throughout the remainder of this Attachment may be DHS standard issued mobile device - initially deployed for use within the United States or "loaner" device separate from the standard issued specifically configured for foreign travel. DHS standard issued mobile device authorized for use domestically and internationally must be configured to mitigate the increased risk inherent with foreign travel.

Authorizing Officials should understand the risks associated with mobile devices regardless of location of use as well as the additional risks associated with their use during international travel and ensure that each risk is measured and mitigated to an acceptable level according to DHS policy. AOs decision to allow DHS standard issued mobile device to be used internationally must take into account Components/Offices mobile ecosystem – Mobile Device Management (MDM) device configurations, Mobile Application Management model, Network Security and Monitoring, and Endpoint Threat Protection capabilities. AOs should also pay particular attention to the conditions in the country(ies) employees will be visiting and should be aware that some countries restrict the use of electronic devices as well as encryption technology.

[1] OMB Circular A-130 defines an Authorizing Official as "a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation."

1.1 SCOPE AND APPLICABILITY

This document provides implementation guidance for DHS-issued mobile devices designated for use by DHS employees on international travel. The guidance pertains to use of mobile devices to access Controlled Unclassified Information (CUI), which includes Personally Identifiable Information (PII), Sensitive Information, and Sensitive PII, as defined in the *DHS Privacy Policy and Compliance Instruction 047-01-011*. It is applicable to all DHS employees, contractors, detailees, and others who will have access to DHS-issued mobile devices while traveling internationally. All categories of personnel are hereafter referred to as "employees".

The policy and accompanying guidance do not apply to special use cases, such as mobile devices used by employees stationed overseas or by those who frequently cross the U.S. border as part of their daily mission work (e.g., Border Patrol agents).

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) is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture (e.g. photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

The document explains security settings and countermeasures for: secure device configuration prior to travel; protections for the device and data during travel; and return, examination, and sanitization of the device upon completion of travel. The techniques described herein are based on *DHS 4300A, Attachment I, Mobile Devices,* and include more stringent restrictions to mitigate the additional risk of using DHS-issued mobile devices while on international travel.

1.2 DHS 4300A POLICY REQUIREMENTS

1.2.1 MOBILE DEVICE SECURITY POLICIES

The policy references described below apply in addition to the policy and guidance provided in this document.

Mobile device security policy and requirements for remote access to DHS networks can be found in DHS 4300A. *DHS 4300A Attachment I, Mobile Devices* and *DHS 4300A Attachments B, Bluetooth Security,* provide policy implementation guidance addressing technology, legal, security, privacy, procedure, and usage issues related to mobile devices.

Policy requirements for international travel with DHS-issued mobile devices are contained in the *International Travel* policy.

1.2.2 SECURITY INCIDENT RESPONSE

DHS Components and Offices need to have an effective reporting and response capability in place before the occurrence of any such security incident, with procedures for reporting and response to incidents that occur when an employee is on international travel. Such procedures and reporting responsibilities, with specific contact information, must be communicated to the international traveler prior to commencement of travel.

1.2.3 SECURITY AWARENESS TRAINING

The goal of security awareness training is to educate DHS users about protecting the confidentiality, integrity, and availability (CIA) of DHS IT assets and data. Prior to travel, the approving authority ensures that employees complete foreign travel training that includes security awareness and cautions employees regarding protection of mobile devices and mobile communications during international travel. The training should also include guidance on how to respond to a request to surrender and/or unlock the device during border crossings and/or airport check points, and how to report incidents involving loss, theft, or suspected compromise of the device or data stored on the device.

The training should also remind employees of their responsibilities to protect sensitive information per DHS Management Directive 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information,* and shall include guidance regarding the types of information considered sensitive that should not be discussed via insecure voice and/or text.

Employees should familiarize themselves with the laws and conditions in the country(ies) they are visiting, including any restrictions on use of mobile devices and encryption technology. The Department of State publishes travel advisories at: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/. The Department of State also provides the Smart Traveler Enrollment Program (STEP), which allows U.S. citizens to enroll with the nearest U.S. embassy or consulate to receive safety and security information on the destination country (https://travel.state.gov/content/passports/en/go/step.html/). The U.S. embassy or consulate in the destination country can provide information on electronic device and/or encryption prohibitions.

1.2.4 OVERSEAS COMMUNICATIONS

Where required or appropriate, all communications outside of the United States and its territories are in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, Information Security Technology, specifically section 12 FAM 643.2-6, Encryption, and section 12 FAM 645.5, Electronic Mail (https://fam.state.gov/FAM/12FAM/12FAM0640.html).

2.0 ROLES AND RESPONSIBILITIES

This section will capture the programmatic and approval responsibilities described in the policy. Examples include, but are not limited to:

- Component Chief Information Officer (CIO) approves use of DHS approved wireless mobile devices based on available resources and nature of the work being done by the employee during the planned international travel
- Components establish a process and issue guidance for distribution and operation of DHS-issued mobile devices while traveling internationally – this includes:
    - Identifying points of contact for approval and forms needed to request device and necessary apps
    - Selecting devices and enterprise mobility management products per *DHS 4300A*
    - Maintaining an inventory of devices and points of contact (POC) 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
- Employee must obtain approval to travel and request authorization to take DHS-issued mobile device on foreign travel[2]
- Supervisors must understand the inherit risk associated with foreign travel and assess if an employee has a mission need to travel internationally with GFE prior to authorizing a request
- Employee must attend foreign travel briefing, which includes security awareness training and guidance on use of mobile devices overseas
- Government employees that require government-issued equipment for any foreign travel must coordinate their network access through their office director for the duration of their trip. Contractors requiring government-issued equipment must contact their Contracting Officer's Representative (COR) for further guidance.
- In accordance with the Office of the Director of National Intelligence Security Executive Agent Directive (SEAD) 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position" (June 12, 2017), and the Department Memorandum, "Foreign Intelligence Threat to DHS" (August 4, 2008), employees:
    - engaged in foreign travel, regardless of clearance level, have limitations and responsibilities related to government-issued equipment.
    - with security clearances and those who hold sensitive positions are required, prior to departure, to report any planned foreign travel for personal or official government reasons and foreign contacts to their respective Chief Security Officers.

[2] Joint Office of the Chief Security Officer and Office of the Chief Information Officer Guidance on Foreign Travel (August 18, 2021)

- If taking a DHS-issued smartphone or tablet on official foreign travel, the employee should contact a U.S. embassy or consulate[3] in the destination country for possible country-specific information regarding prohibitions against electronic devices and/or encryption technology.

3.0 FOREIGN THREAT OVERVIEW

The threats described in *4300A Attachment I, Mobile Devices* are relevant regardless of location of the accompanying mobile device and the user; the following sections provide additional security awareness considerations for AOs and users during international travel.

The presence of DHS employees traveling on official business in a foreign country may be known to the country's officials prior to arrival or upon arrival at the border, e.g., if the travel requires issuance of a visa or if the traveler carries an official U.S. passport. In the event the traveling DHS employee does not have an official U.S. passport (e.g., employee is traveling on a tourist passport or visa), advance notice is not generally provided, and the destination country's officials may/may not be aware of the DHS employee's arrival at the border. DHS employees traveling on a tourist passport or visa who conduct any official business while on travel shall take any/all precautions as though they were traveling on official business.

As representatives of the U.S. government, DHS employees 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 the mobile device attacked overseas varies based on the country visited, who the employee is or their position within DHS, and how interested state and non-state actors are in DHS and/or the employee's work. Employees on international travel should assume that their communications and activities are being monitored and conduct themselves accordingly.

3.1 MOBILE NETWORK THREATS

Mobile devices will connect to any available network, including untrusted Wi-Fi networks or foreign-owned/operated cellular networks. This always-on connectivity presents heightened risk to DHS users and data when the devices are used overseas. Wireless communications provide limited security from interception, jamming, or other threats. The use of proper procedures and specific technology can reduce the likelihood that wireless communications are exposed; however, the technology may not be available on DHS GFE consumer mobile devices.

Eavesdropping on Wi-Fi, cellular and Bluetooth wireless communications with commercially available equipment is common. Any Wi-Fi network, whether free or paid for, that is outside the control of the U.S. government should be considered untrusted and subject to monitoring. Rogue base stations can force a user's device to downgrade to less secure Wi-Fi protocols and thereby enable a man-in-the-middle attack. Interception of cellular traffic is also possible by monitoring cellular towers and by other man-in-the-middle techniques.

International mobile (cellular) networks may be owned or controlled by the host government, which can monitor all communications to and from the device. Foreign

[3] U.S. Department of State - Official list of U.S. Embassies, Consulates and Domestic Missions. (https://www.usembassy.gov).

mobile network operators 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 mobile operators' core networks overseas. SS7 has a flat trust model (all operators are trusted) and this trust 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 user bank accounts.

3.2 LOCATION TRACKING

Geolocation and timing services are essential to the operation of any cellular network 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.

3.3 MALWARE AND SURVEILLANCE-WARE

There is an active surveillance industry that sells products and services to state and non-state 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., executives) and install malware to compromise the device or attack DHS backend systems, or to install surveillance-ware which can intercept calls and text messages or turn on the mobile device's camera or microphone without the user's knowledge.

Physical access to the mobile device, e.g., if required to surrender the device during a border crossing, or if left unattended in a hotel room or other location, is a direct vector for delivery of such malware to the device.

Carriers controlled by foreign governments can push malware directly to the mobile device. This 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 the mobile device.

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

Minimizing the sensitive DHS 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.

Employees should understand the visited country's laws regarding border searches; if the traveler refuses to comply with the request, border officials may seize the device. 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, employees should immediately power down the device and report the incident as soon as feasible to their immediate supervisor, who follows established incident reporting procedures outlined in *4300A Attachment F – Incident Response* which includes contacting the Component Security Operations Center (SOC). The same procedures apply if the device is seized and not returned; immediately report the incident to the Component SOC, and to the local U.S. embassy or consulate.

4.0 SECURING THE DEVICE PRIOR TO INTERNATIONAL TRAVEL

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

All security requirements specified in *DHS 4300A Attachment I, Mobile Devices* shall be followed for the specially configured devices. Critical techniques to mitigate risks of mobile devices that remotely access DHS systems and data from overseas include: central management of the device and applications; baseline secure configuration with unneeded features and capabilities disabled; strong authentication of the user and the device; DHS policy-compliant password to unlock the device; minimum apps and data required for official business; protection of data at rest and in transit; monitoring the device for deviation from security policy and for indicators of mobile threats; and physical security. Secure Digital (SD) cards or other external media should not be used/issued with the device.

4.1 MANAGE MOBILE DEVICES AND APPLICATIONS

All DHS-issued mobile devices shall be managed and monitored by a DHS Mobile Device Management (MDM)/Enterprise Mobility Management (EMM) system. An MDM/EMM allows DHS 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. All mobile devices must be accounted for in a Federal Information Security Modernization Act (FISMA)-inventoried system.

The AO shall ensure that the mobile device is running the most current mobile operating system and the current version and security patches for installed apps and firmware. An up-to-date operating system is the first line of defense against threats to the device. While it may seem more cost efficient to use older smartphones as DHS-issued mobile devices, such devices may not support the latest mobile operating system. In addition to patching vulnerabilities, new operating system versions often bring security architecture improvements that provide resilience against as yet undiscovered vulnerabilities or weaknesses.

4.1.1 INSTALL MINIMUM SET OF MANAGED MOBILE APPS

DHS mobile applications configured on DHS-issued mobile device should be managed by DHS. To reduce the risk of exposure of DHS and employee personal data, the AO must determine what mobile apps and data shall be installed or accessible to the employee during foreign travel (e.g., secure email, secure browser, office productivity, Mobile Threat Defense protection, etc.). The devices shall be configured to disallow user download and installation of apps from unofficial app markets or unknown sources. To reduce the amount of email data stored on the device, AOs may consider limiting mailbox size and access to enterprise email archives or issuing the employee a separate temporary internal email account for the mobile device. AOs may also consider using virtual mobile infrastructure/virtual desktop infrastructure to minimize the data and applications on the device.

4.1.2 ENFORCE AUTHENTICATION REQUIREMENTS

The AO shall ensure that authentication and access controls are required to access the device and the data on the device. Device unlock shall be configured to require a strong password known only by the user. At the discretion of the AO, biometric (e.g., fingerprint, face image, iris scan) may be enabled for device unlock. Biometric characteristics are not considered private and government officials can compel users to unlock a device with their fingerprint, iris scan, or other biometric identifier.

Email and any other allowed DHS mobile apps shall require user authentication in compliance with the requirements defined in *the Identification and Authentication Control Family* of *DHS 4300A*. Access to the DHS network shall require mutual identification and authentication of both the user and the device.

Users should be instructed to choose different passwords for use on their DHS-issued mobile device while on international travel than those used when in the continental United States and US territories.

4.1.3 PROTECT DATA AT REST AND IN TRANSIT

All data on mobile devices shall be encrypted using Federal Information Processing Standard (FIPS) 140-2 validated encryption schemes; passwords to encrypt the data shall comply with the requirements defined in *Identification and Authentication Control Family* of *DHS 4300A*. 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 AO shall ensure that the device's find my phone and remote wipe features are enabled so the MDM/EMM can perform remote wipe to protect data from unauthorized access in the event of device loss, theft, or suspected compromise.

4.1.4 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 wireless attacks. Because they are not controlled by DHS, foreign networks introduce security risks when used by DHS personnel. Cellular infrastructure may not be owned by the mobile network carrier; may be controlled by a foreign government; and 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.

For all wireless data access, the device shall be configured to use the appropriate level of encryption to protect data in transit based on the FIPS 199 categorization of data sensitivity, e.g., per-app Virtual Private Network (VPN). If communications with external networks are allowed and cannot be attained through the DHS network, then browser communications shall be secured with the HyperText Transfer Protocol Secure (HTTPS) protocol.

For devices issued to executives and authorized personnel, the AO may consider including an additional layer of separation between the mobile device and foreign Wi-Fi or cellular networks through use of a portable wireless access point ("hotspot"). The hotspot device shall be secured in accordance with Wi-Fi guidance in *DHS 4300A Attachment I, Sensitive Mobile Devices.*

4.1.5 DISABLE NON-ESSENTIAL 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, these capabilities shall be disabled: infrared, Bluetooth (see DHS *4300A Attachment A, Bluetooth Security)*, Near Field Communication (NFC), and other unneeded tools and applications, such as those pre-installed by the mobile device vendor or the cellular carrier.

Turning off Wi-Fi through MDM policy is recommended (unless using a portable wireless access point with the mobile device); at minimum, settings to automatically join Wi-Fi networks shall be disabled. Location services should be disabled for mobile apps that are not mission essential.

4.1.6 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 must be coordinated with the DHS Office of the Chief Information Security Officer (OCISO).

4.2 INSTALL MOBILE THREAT DEFENSE (MTD) PROTECTION

Mobile devices provide ready access to remote email, files, and other business 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 DHS data.

Information security mechanisms for DHS enterprise IT systems and services should be used to protect mobile devices. For example, email should be scanned at the DHS email servers before it is delivered to the mobile device. The MDM/EMM will check device configuration and compliance with device security policy when the employee connects to email or other DHS resources; however, these checks may occur infrequently during travel.

As an additional countermeasure to detect anomalous behavior in real-time, mobile threat defense protection shall 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 MDM/EMM administrator and the user. The software should be configured to remediate malicious behavior, either independently or via integration with the MDM/EMM. The information collected by mobile endpoint protection software should be limited to the minimum data necessary to perform its function.

Approval of mobile threat defense protection software for real-time security monitoring of the mobile device is the overall responsibility of the AO.

More information about Mobile Threat Defense protection can be found in *NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise*.

4.3 CAPTURE DEVICE BASELINE CONFIGURATION

Following provisioning and configuration of the mobile device, the device administrator should use the Traveler Verified Information Protection (T-VIP) or a similar capability to capture the expected baseline configuration of the loaner mobile device prior to issuance to an employee. Upon return, the device will be examined, and the actual baseline should be compared against the expected baseline to detect malware or unauthorized modifications of device settings, configuration, software, firmware, hardware, and data.

5.0 PROTECTING THE DEVICE AND DATA DURING TRAVEL

Travelers need to be especially vigilant and wary to mitigate loss and theft of the device; eavesdropping of conversations and screen activity, and data; and other vulnerabilities to the CIA of information stored or accessed on the mobile device for the duration of their travel. Traveling employees are responsible for complying with the rules of behavior and exercising security and safety awareness while on travel.

5.1 MAINTAIN POSSESSION OF DEVICE

Employees must maintain possession of the DHS-issued mobile device at all times during international travel, and must never leave the device unattended in a vehicle, hotel room, conference room, work area, or other location. Devices should be turned off when not in use; this reduces battery drain, location tracking, and brute force password attacks. Users shall transport the mobile device in carry-on luggage rather than checked baggage and should maintain awareness of the device when going through X-ray machines and other physical security examination devices.

Travelers attending meetings or visiting secured locations where electronic devices are not allowed should not bring the devices with them. Employees should not hand over a DHS-issued device unless specifically required to do so. Before turning it over, e.g., to border agents, or depositing it in a temporary storage location, employees should first turn the device off and then remove and keep the battery (if applicable) and Universal Integrated Circuit Card (UICC), (generally referred to as a SIM card) from the mobile device. As soon as the device is returned, users will inspect it for any obvious signs of tampering before replacing the battery and UICC and powering it on.

5.2 TURN OFF WI-FI AND BLUETOOTH

Unless mission essential, turn off Bluetooth and ensure that it remains disabled. If Bluetooth is allowed, follow the guidance in *DHS 4300A Attachment A, Bluetooth Security*. If Wi-Fi use is allowed, turn it off when not in use; the constant pinging of radios can be used to locate the employee, and turning it off will help conserve battery life. When these services are turned on the radios are constantly searching for Wi-Fi networks to connect to.

Wi-Fi networks, once joined, are then saved by default. If a Wi-Fi network is used while traveling, this and any Wi-Fi network should be removed from the list of previously joined networks. Travelers shall manually remove all joined Wi-Fi networks after use.

In some countries, these networks are controlled by security services; many free and public Wi-Fi networks do not require user authentication and do not encrypt data communications, leaving data exposed. Wi-Fi networks provided by airports, hotels, or businesses may require a passcode for authentication, however, these are untrusted and all traffic may be monitored.

5.3 BE WARY OF 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 carrier informing them of local mobile and data rates. The messages are effective because mobile device users are familiar with them and may expect them when they activate their phone. Employees should recognize these attempts and never click on such links, nor should employees install any enterprise certificates.

Other attacks that may be less obvious are firmware or operating system update notifications that arrive as the traveler enters the country. 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 communications and user activities. Since the device was configured and updated to the most recent operating system versions and apps prior to delivery to the employee, there should be no need to update it during travel; if an emergency patch or update is necessary, notification should come via the DHS MDM/EMM.

5.4 VERIFY LOCATION SERVICES SETTINGS

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

5.5 REPORT SECURITY INCIDENTS IMMEDIATELY

DHS employees shall immediately report incidents involving loss, theft, compromise or suspected compromise of the DHS-issued mobile device during international travel per *DHS 4300A Attachment F, Incident Response* . Employees shall also immediately report suspected loss, compromise, or unauthorized disclosure of CUI or PII during travel. DHS employees who are required to surrender the DHS-issued device for inspection at customs or a border crossing will not disclose any passwords used for encryption or access control. DHS employees who are coerced into revealing mobile device decryption or unlock passwords will immediately report the incident Component Security Operations Center (SOC) and change the passwords as soon as possible.

6.0 RETURN AND INSPECTION OF THE DEVICE AFTER TRAVEL

Upon completion of international travel, the employee may be required to return their DHS-issued mobile device, any portable media (e.g., SD card), and device passcodes to the device issuing office per organizational policy and at the discretion of the AO. The device shall not be connected to a DHS network. The device should be inspected using T-VIP or a similar forensic capability. This process will examine and compare the actual device configuration, software, firmware, and hardware to the pre-trip or expected baseline to determine if there have been modifications, additions, or deletions to the device from its trusted state.

The AO is responsible for rendering a risk management decision on reset/reuse of the device based on the results of the digital media analysis and policy. Data on the 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 management utility permanently remove files. On completion of device examination and sanitization (or destruction), the loaner device inventory will be updated to reflect its availability and the international service plan will be discontinued per Component policy.

APPENDIX A—ACRONYMS

Acronym	Definition
2G	Second Generation
3G	Third Generation
4G	Fourth Generation
AO	Authorizing Official
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
EMM	Enterprise Mobility Management
FAM	Foreign Affairs Manual
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
MAM	Mobile Application Management
MDM	Mobile Device Management
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OCISO	Office of the Chief Information Security Officer
PII	Personally Identifiable Information
POC	Point of Contact
SD	Secure Digital
SIM	Subscriber Identity Module
SMS	Short Message Service
SS7	Signaling System 7
STEP	Smart Traveler Enrollment Program
T-VIP	Traveler Verified Information Protection
UICC	Universal Integrated Circuit Card
VPN	Virtual Private Network