IT/IM DIRECTIVE PROCEDURE

Directive No: CIO 2150-P-18.3

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

International Travel Procedures for Mobile Devices

1. PURPOSE

To safeguard Environmental Protection Agency (EPA) information and systems for all employees, contractors, and other users while on international travel or on travel to specifically designated locations within the United States and territories that are not owned or controlled by the United States (e.g., foreign embassies).

2. SCOPE

This procedure covers all EPA-issued mobile devices, such as laptops, tablets (notebook), memory drives, portable Wi-Fi, cell phones, and smartphones that store, process, transmit, or receive EPA information when such devices are used or carried on international travel.

Direct travel to and from and within U.S. territories and commonwealths is not considered international travel.

This procedure applies to all EPA employees, contractors, and other users of EPA information and information systems.

3. AUDIENCE

The audience is all EPA employees, contractors, and other users of EPA information and information systems.

4. AUTHORITY

The information directive is issued by the EPA Chief Information Officer (CIO), Pursuant to Delegation 1-19, dated 07/07/2005. Additional legal foundations for the procedure include:

- National Institute of Standards and Technology (NIST) Special Publication 80053-Rev 5 *Security and Privacy controls for Information Systems and Organizations*
- EPA CIO 2150.3, *Environmental Protection Agency Information Security Policy*, August 6, 2012 and all subsequent updates or superseding directives

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act
- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)

5. PROCEDURE

General:

1) Do not take mobile devices if the mission can be accomplished without them.

2) Take the minimum amount of information necessary to accomplish the mission. This includes sensitive contact information and non-electronic media.

3) Save all EPA information from mobile devices to appropriate EPA systems prior to travel.

4) EPA-issued mobile devices shall only be used for government-authorized uses.

5) While on international travel to high-risk locations, non-EPA issued mobile or other devices shall not be used to conduct official EPA business or to store, process, or transmit EPA information and shall not be connected to EPA's systems. Use of other U.S. Government resources (e.g., Department of State or Department of Defense) is permitted for operational necessity and emergencies.

6) Specially-configured, EPA-issued mobile devices are recommended for all official international travel, but are not required for international travel to locations not identified as high risk. Use of standard EPA mobile solutions is acceptable in cases where specially-configured devices are not required. Conditions may exist, as determined by the EPA Office of Information Security & Privacy (OISP) where specially-configured devices are required when international travel locations are not otherwise identified as high risk. Although, users will have access to M365 apps (e.g. OneDrive, Teams, SharePoint), some features such as Bluetooth, Facetime, and SMS text messaging will be disabled on a specially-configured loaner device.

7) Users shall be allowed to take specially-configured, EPA-issued mobile devices to enable them to conduct official EPA business while on personal travel to high-risk international locations. However, Senior Resource Official (SRO) approval is required for conducting official government business while on personal international travel. For additional questions, the user shall consult with their manager.

8) Users conducting official EPA business on mobile devices during travel must export and save those records to an official EPA recordkeeping system or to their epa.gov email address upon their return to fulfill the requirements of the Federal Records Act (44 U.S.C. § 2911) and EPA Records Management policy (CIO 2155.5). For records management questions, users shall contact Records Liaison Officer or the Records Program at records@epa.gov .

Additionally, users must preserve any information transmitted or stored on the mobile device that relates to a matter identified in a litigation hold or is subject to preservation requirements, which may arise under the Federal Records Act, FOIA, Privacy Act, congressional requests, litigation holds and court preservation orders (collectively, hereinafter "Records and Legal Hold Information"). Litigation Hold Custodians: To review legal hold obligations, users shall access their personal litigation hold custodian portal in Relativity Legal Hold to review their legal hold obligations. To locate the link users custodian portal, users should search their Outlook for an email from EPA_Legal_Hold@epa.gov. If the user cannot locate an email from EPA_Legal_Hold@epa.gov that contains their personal custodian portal link, they should contact EPA_Legal_Hold@epa.gov to request a new personal portal link.

9) To determine if specially-configured devices are needed,, users shall submit an "International Travel Loaner Laptop/Mobile Device Request" at least two weeks in advance of their last scheduled day in the office (or their current telework location). If the location is determined to be low risk, the traveler may carry their currently assigned agency laptop, iPhone and/or iPad.

10) Permission to travel internationally on EPA business is managed via the Fast International Approval of Travel (FIAT) system. Contact an International Travel Coordinator (ITC) for information about accessing FIAT. (Users may submit the request for loaner devices prior to or in parallel to the FIAT request.) For more details, users should access the International Travel site..

11) The loaner request will route to the appropriate Information Security Officer (ISO)for awareness and review. The Office of Information Security and Privacy (OISP) will determine the risk of the listed locations to include any layovers during the trip. OISP will consult, if needed, with the Office of National Security (ONS). Based on OISP designation of locations (high or low risk), the request will be routed appropriately, and the requestor/traveler will be notified.

12) For high risk locations, an email is sent to the traveler/requestor with information about the loaner laptop and instructions to place an eBusiness order for the loaner mobile device (e.g. iPhone and iPad). Additionally, the traveler will be required to review

the International Travel to High Risk Location training prior to ordering a loaner device from eBusiness. If the traveler has not taken the training when the order is placed into eBusiness then the order will be canceled, and a new order will be required after the training is taken. The training takes less than 5 minutes and will only be required once a year.

And for low risk locations, an email is sent to the traveler/requestor notifying them that they can carry their current laptop and mobile device (e.g. iPhone or iPad) and instructions for adding an international rate plan.

13) Users on all international travel shall immediately report the loss, theft, compromise or suspected compromise of EPA-issued mobile devices or EPA information to their ISO, supervisor, and Enterprise IT Service Desk (EISD). 16) Users shall physically secure mobile devices and information while on travel. For example:

a)Do not store devices in checked baggage.
b)Use digital signature and encryption capabilities when possible.
c)Do not leave devices or sensitive information unattended in public places (e.g. airports, restaurants, conference meeting rooms).
d)Guard against eavesdroppers and shoulder surfers.
e)Secure laptops in hotel rooms with a locking device.
f)Ensure devices are lock when not in use

14) The Director of the Office of Information Technology Operations (OITO) shall develop and maintain processes and minimum configuration standards for all specially configured devices.

15) Senior Information Officials (SIO) shall ensure supervisors or managers of IT help desks and IT staffs providing support for specially-configured devices held in reserve, develop, maintain current, implement and publish local supplemental procedures, standards or guides for maintaining devices through their life cycle and for issuing, tracking, collecting, sanitizing and transferring information to users. (Note: Program Offices are supported by OMS' Enterprise IT Service Desk (EISD), therefore, specially-configured devices are requested, stored, managed, and issued by ~~EISD~~ OMS)

a)Local procedures, standards or guides shall include specifications on how approved storage devices will be used with mobile computing devices such as laptops, tablets and smartphones to ensure information is only transferred to or from approved and properly configured devices and only using approved methods.
b)Local procedures, standards or guides shall include specifications on how computing devices will be connected to communication devices such as

smartphones to ensure information is only transmitted or received using approved methods and only with approved and properly-configured devices.

16) SIOs shall develop, document, and implement a process to ensure the international procedures are being followed.

a) An example of a process is as follows:

i) Someone is designated to monitor the Fast International Approval and Tracking (FIAT) Database for International Travelers each month.

ii) The monitor contacts travelers identified in FIAT to determine their IT equipment needs for their trip.

iii) The monitor enters into and tracks the pertinent information for each traveler using a spreadsheet.

iv) The monitor distributes the information to appropriate individuals according to IT needs.

v) If a laptop is needed, then:

(1) The traveler submits an "International Travel Loaner Laptop/Mobile Device" request via ServiceNow to determine if the location is high risk. If high risk, a specially-configured loaner laptop is required.

(2) Once the loaner laptop is received, the traveler works with the help desk to transfer work related files needed for their trip to the loaner laptop prior to departure.

(3) Upon return, the traveler shall immediately coordinate the return and processing (e.g., transferring documents from the laptop) of the laptop with their help desk

vi) If an iPhone or iPad is needed, an order is placed within eBusiness by the Working Capital Fund manager in two ways:

(1) For travelers who currently have an Agency issued device, a request is entered into eBusiness to have the International Data Package added to their device for the duration of their trip.

Note: For those who frequently travel outside of the country, this package is not removed.

(2) For travelers who do not have an Agency issued device, a request is entered into eBusiness to order a Loaner International Device for the duration of the traveler's trip. This request is submitted two weeks prior to the traveler's departure date to ensure that it arrives in time. Mobile devices taken to high-risk locations shall resist physical tampering and unauthorized information transmissions and transfers to and from the devices.

a. An example of resisting physical tampering is the automatic erasure of information stored on a USB device when the case is opened.
b. Examples of resisting unauthorized information transmissions (e.g. malware, transfers) are turning off Wi-Fi and Bluetooth capabilities

Laptops, Handheld Mobile Devices, and Mobile Storage Devices:

Note: Also applies to Notebooks, Tablets and similar devices.

1) When in a travel status for any international travel, users:
    a. Shall manually turn off the wireless access when not in use and turn it on only when needed.

2) Upon return to work from international travel to high risk locations, users:
    a. Shall sign the MD Acknowledgement Form certifying that they have complied with records and litigation hold obligations.
    b. Shall send the signed MD Acknowledgement Form to their WCF Manager so they can attach the form with the eBusiness cancellation.
    c. Shall contact their local IT help desk or IT staffs issuing specially configured devices immediately to arrange for the pickup and sanitizing of loaner laptops. If there is information on loaner laptops users need or is subject to an active litigation hold, users should request the information be removed and provided to them prior to laptops being sanitized (wiped).
        i) Help desk personnel and IT staffs shall ensure information is malware-free prior to providing it to the user.
        ii) If malware is detected and cannot be removed or it is suspected it has not been removed, help desk personnel and IT staffs shall contact users' ISO for guidance. ISOs shall coordinate with the EPA Computer Security Incident Response Capability (CSIRC) for a solution.
    d. Shall not connect loaner devices to any EPA system or network.
    e. Users shall not transfer data to any EPA system other than as authorized for travel.

Portable Wi-Fi & Mobile Hotspot:

1) When in a travel status for any international travel, users:
   a) Shall only use specially-configured, EPA-issued mobile devices that are authorized for Wi-Fi connection use.
   b) Shall manually turn off the wireless access when not in use and turn it on only when needed.
   c) Shall not connect loaner devices to any EPA system other than the ones authorized for use on travel (e.g., laptop or smartphone).
   d) Shall not transfer data to any EPA system other than as authorized for travel.

6. ROLES AND RESPONSIBILITIES

If individuals choose to re-delegate or to assign responsibilities, that re-delegation or assignment must be documented in writing if not already re-delegated in EPA policy.

Senior Information Officials (SIO)

1) Ensure supervisors or managers of IT help desks and IT staffs, within the SIO's area of responsibility, provide support for specially-configured devices held in reserve and develop, maintain, implement and publish local supplemental procedures, standards or guides for:
   a) Maintaining devices through their life cycle, and for issuing, tracking, collecting, sanitizing and transferring information back to users.

2) Ensure a process is developed, documented and implemented to ensure international procedures are followed.

Note: Program Offices are supported by OMS' Enterprise IT Service Desk (EISD), therefore, specially-configured devices are requested, stored, managed, and issued by OMS).

Chief Information Security Officer (CISO)

1) Adjudicate travel locations in terms of 'High' or 'Low' risk.

Collaborate with EPA ONS on cyber intelligence and risk determinations.

Director of Office of Information Technology Operations (OITO)

1) Develop and maintain processes and minimum configuration standards for all specially configured devices.

Information Management Officers (IMO)

1) Provide user guidance on processes and directives.

Information Security Officers (ISO)
1) Review and provide concurrence of the international travel laptop/mobile device loaner request in ServiceNow.
2) Provide user guidance on processes and directives.

Senior Resource Official
1) Review and approve request to conduct official government business (telework) while on personal travel.

Senior Intelligence Advisor/EPA Federal Senior Intelligence Coordinator, EPA Office of National Security (ONS)
1) Provide guidance and advice to OISP, when needed, on international travel requests.

WCF Manager
1) Ordering/approving the needed international equipment and canceling the order once the traveler returns.

IT Help Desks and IT Staffs Providing Support for Specially Configured Devices Held in Reserve
1) Develop, maintain publish and implement local supplemental procedures, standards or guides for maintaining devices through their lifecycle and issue, track, collect, sanitize and transfer information back to users.

7. RELATED INFORMATION

- Personal Computer Configuration and Management Standard, CIO 2122-S-02.2, 5/8/23, and all subsequent updates or superseding directives.
- EPA Information Procedures: CIO-2150.4-P-01.4, Mobile Computing Management Procedures,November 21, 2023.
- Applicable NIST Special Publication (SP) and Federal Information Processing Standards (FIPS) as updated or superseded to include but not limited to: NIST SP 800-147, Basic Input/Output System (BIOS) Protection Guidelines
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

- NIST SP 800-121, Guide to Bluetooth Security
- NIST SP 800-114, User's Guide to Telework and Bring Your Own Device (BYOD) Security
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- NIST SP 800-88, Guidelines for Media Sanitization
- NIST SP 800-53, REV5, Recommended Security Controls for Federal Information Systems and Organizations
- FIPS 140-2, Security Requirements for Cryptographic Modules
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- Supplemental procedures, standards and guides developed to implement this procedure.

8. DEFINITIONS

- **High-risk location:** location where the threat of cyber or electronic surveillance presents elevated risks and requires additional precautions.
- **Mobile device:** portable cartridge/disk-based, removable storage media (e.g., floppy disks**,** compact disks, USB flash drives, external hard drives and other flash memory cards/drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, audio recording devices and portable Wi-Fi devices).
- **Specially-configured devices:** devices that have additional controls to help mitigate risks associated with cyber or electronic surveillance.

9. WAIVERS

There are no waivers allowed for this international travel procedure.

10. DIRECTIVE(S) SUPERSEDED

EPA Information Procedures: CIO 2150-P-18.2, International Travel Procedure for Mobile Devices, December 29, 2016.

11. CONTACTS

For further information, please contact your Information Security Officer. You also may contact the Office of Mission Support, Office of Information Technology Operations.

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2024.11.21 09:35:30 -05'00'

Vaughn Noga, Chief Information Officer and Deputy Assistant Administrator for Information Technology and Information Management