INFORMATION DIRECTIVE
PROCEDURE

International Travel Procedure for Mobile Devices		
Directive No.: 2150-P-18.2	CIO Approval: 12/29/2016	Transmittal No.: 17-004c

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

International Travel Procedure 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. BACKGROUND

Mobile devices extend the virtual boundary of EPA systems and add risk that must be properly mitigated. The use of mobile devices to transmit or receive information via telecommunication networks presents security risks due to the susceptibility to eavesdropping, interception of transmitted information and introduction of malware. Such risks are higher while on international travel in locations where telecommunication networks are owned or controlled by the host government because of the ease in which the host government can monitor transmissions. This also applies to visits and meetings at facilities within the United States and U.S. territories that are owned or under the control of non-U.S. entities. The use of mobile devices outside EPA facilities that provide adequate physical protections also present higher risks due to loss, theft and tampering. As with risks associated with transmitted information, in some international locations these risks are increased even more. The use of mobile devices presents different risks, when compared to the use of non-mobile devices, which require different or modified controls and procedures, such as this one for international travel.

5. 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 800-53-Rev 4, *Recommended Security Controls for Federal Information Systems and Organizations*, and all subsequent updates or superseding directives
- 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.)

6. 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) When applicable, remove the batteries from mobile devices when not in use.
5) EPA-issued mobile devices shall only be used for government-authorized uses.
6) 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.
7) 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.
    a) Conditions may exist, as determined by the EPA Office of Homeland Security (OHS), where specially-configured devices are required when international travel locations are not otherwise identified as high risk.
8) When traveling internationally to high-risk locations or locations identified by OHS for any reason, only specially-configured, EPA-issued mobile devices are authorized for use for EPA business.

9) 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.

10) When traveling internationally to high-risk locations or locations identified by OHS, users shall be provided mobile devices specially-configured for international travel to high-risk locations.

    a) To obtain specially-configured devices, users shall follow local procedures. Users can contact their supporting information technology (IT) help desk. For example, Headquarters users contact the Headquarters help desk, Information Security Officer (ISO) or Information Management Officer (IMO) for local procedures.[1]

        i) Offices and regions have the option to maintain a reserve of specially-configured devices to issue to personnel traveling to high-risk locations. Devices maintained in reserve shall comply with all applicable EPA Policy, Procedures, Standards, and Guidance.

            (1) Laptops, laptop hard drives, Universal Serial Bus (USB) storage devices, secure digital (SD) cards, portable Wi-Fi (hotspots), tablets (notebook), and mobile or smart phones are examples of devices that may be specially-configured and held in reserve.

11) All users shall refer to the Office of International and Tribal Affairs' (OITA) International Travel website for additional guidance. Users shall coordinate with their ISO to determine if specially-configured, EPA-issued devices are required for their travel.

12) ISOs shall contact the EPA Senior Agency Information Security Officer (SAISO) with the user's travel request information to determine whether a specially-configured, EPA-issued mobile device is required.

    a) Minimum travel information required:

        i) Position (e.g., Office Director, Assistant Administrator)

        ii) Travel date(s) to include month, day, and year

        iii) Travel destination(s) to include city and country

        iv) Reason for travel (e.g., Wastecon Conference)

13) The SAISO will forward the travel information to OHS for review.

14) The SAISO shall develop and maintain a list of high-risk locations. The list shall be updated annually.

15) The SAISO will provide the list of high-risk locations to OHS.

16) OHS will review international travel requests and provide input to the SAISO as necessary. OHS will inform travelers directly or inform the SAISO whether specially-configured devices will be required for their travel. If OHS informs the SAISO of their determination, the SAISO will inform the ISO. The ISO will inform the traveler of the final determination.

17) Users on all international travel shall immediately report the loss, theft, compromise or suspected compromise of EPA-issued mobile devices or EPA information via established incident reporting procedures and to the local U.S. Embassy.

[1] Appendix A: International Travel Procedure for Mobile Devices Process *shows a high level process for obtaining specially configured devices.*

18) 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.
19) The Director of the Office of Information Technology Operations (OITO) shall develop and maintain processes and minimum configuration standards for all specially configured devices.
20) 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.
    a) Local procedures, standards or guides shall include specifications on how storage devices will be used with mobile computing devices such as laptops 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 used with communication devices such as smartphones to ensure information is only transmitted or received using approved methods and only with approved and properly-configured devices.
21) 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 organization's ISO submits a request to the Program Manager for the help desk provider to obtain a properly secured loaner laptop.
            (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 with the Working Capital Fund by the organization’s Service Agreement originator 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 are turning off Wi-Fi and Bluetooth capabilities.

c. An example of resisting unauthorized information transmissions (e.g., malware, transfers) is locking an SD card to prevent writing to the card.

Laptops:

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 contact their local IT help desk or IT staffs issuing specially configured devices immediately to arrange for the pickup, scanning and sanitizing of loaner laptops. If there is information on loaner laptops users need, users can request the information be removed and provided to them prior to laptops being sanitized.

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.

b) Shall not connect loaner devices to any EPA system other than the ones authorized for use on travel (e.g., laptop or smartphone).

c) Shall not transfer data to any EPA system other than as authorized for travel.

Handheld Mobile Devices (e.g., Personal Digital Assistant (PDA), smartphone and similar devices):

1) Upon return to work from international travel to high-risk locations, users:
   a) Shall contact their local IT help desk or IT staffs issuing specially-configured devices immediately to arrange for the pickup, scanning and sanitizing of loaner devices. If there is information on loaner devices users need, users can request the information be removed and provided to them prior to devices being sanitized.
      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 a user's ISO for guidance. ISOs shall coordinate with the EPA CSIRC for a solution.
   b) Shall not connect loaner devices to any EPA system other than the ones authorized for use on travel (e.g., laptop or smartphone).
   c) Shall not transfer data to any EPA system other than as authorized for travel.

Mobile Storage Devices (e.g., USB memory sticks, hard drives, SD cards and similar devices):

1) Upon return to work from international travel to high-risk locations, users:
   a) Shall contact their supporting IT help desk or IT staffs issuing specially configured devices immediately to arrange for the pickup, scanning and sanitizing of loaner devices. If there is information on loaner devices users need, users can request the information be removed and provided to them prior to devices being sanitized.
      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 a user's ISO for guidance. ISOs shall coordinate with the EPA CSIRC for a solution.
   b) Shall not connect loaner devices to any EPA system other than the ones authorized for use on travel (e.g., laptop or smartphone).
   c) 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.

i) Users shall disable ad hoc connections and disallow automatically connecting to wireless network.

ii) Users shall use a Virtual Private Network (VPN) connection with strong Encryption (e.g., Wi-Fi Protected Access 2 (WPA2) 256-bit key).

iii) Users shall ensure that they are connected over the Secure Sockets Layer (SSL) and using at least two factor authentication for the destination website.

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.

7. 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.

Senior Agency Information Security Officer (SAISO)

1) Determine and maintain a list of high-risk international travel locations.
2) Update the list of high-risk international travel locations annually.
3) Provide a determination on high-risk international travel locations to ISOs.
4) Provide the list of high-risk international travel locations to OHS.
5) Report any suspected compromise or anomalies to OHS.

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) Obtain and provide traveler information to SAISO.
2) Obtain determination of high-risk international locations from the SAISO and provide to traveler.
3) Provide user guidance on processes and directives.

Senior Intelligence Advisor/EPA Federal Senior Intelligence Coordinator, EPA Office of Homeland Security (OHS)

1) Review international travel requests and determine if conditions exist that require specially configured devices for travel locations.
2) Inform the SAISO or traveler of the need for specially configured devices for particular travel requests.
3) Determine the conditions and/or circumstances under which specially configured devices shall be issued for use within the United States and territories.
4) Monitor and analyze any known or suspected compromises or anomalies reported by the Office of Environmental Information (OEI).

IT Help Desks and IT Staffs Providing Support for Specially Configured Devices Held in Reserve

1) Develop, maintain current, publish and implement local supplemental procedures, standards or guides for maintaining devices through their life cycle and issue, track, collect, sanitize and transfer information back to users.

8. RELATED INFORMATION

- Personal Computer Configuration and Management Standard, CIO 2122-S-02.0, 10/1/10, and all subsequent updates or superseding directives.
- EPA Information Procedures: CIO-2150.4-P-01.1, Mobile Computing Management Procedures, December 6, 2013.
- 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 on Cell Phone and PDA Security
  - 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 Securing External Devices for Telework and Remote Access
  - NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
  - NIST SP 800-88, Guidelines for Media Sanitization
  - NIST SP 800-64, Rev. 2, Security Consideration in the System Development Life Cycle
  - NIST SP 800-53, Rev4, 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.

9. 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.

Abbreviations including acronyms are summarized in *Appendix B: Acronyms & Abbreviations*.

10. WAIVERS

Waivers may be requested from the SAISO by submitting a justification based on:

- substantive business case need(s)
- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The SAISO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director of OITO shall coordinate to maintain a central repository of all waivers.

11. MATERIAL SUPERSEDED

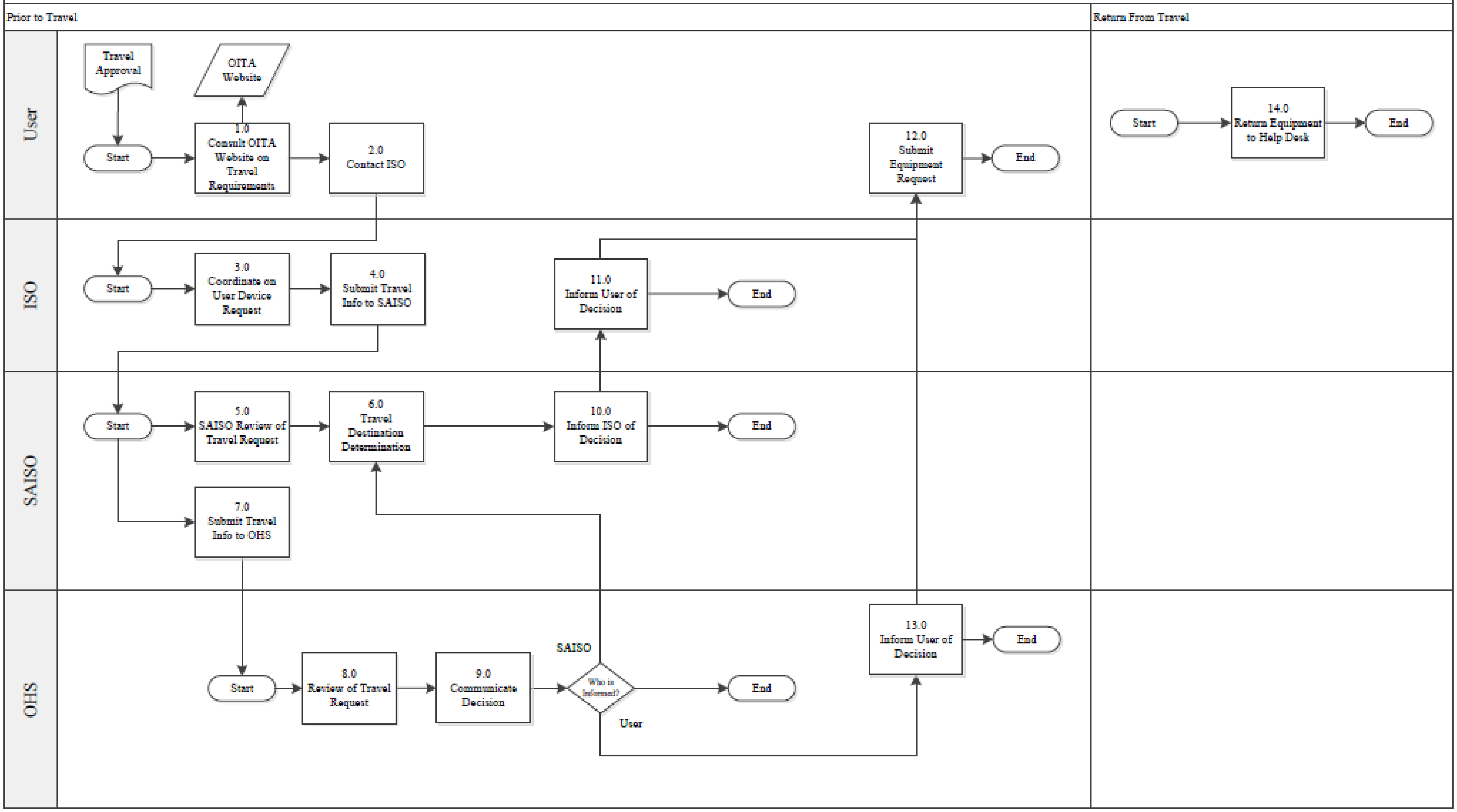
EPA Information Procedures: CIO-2150.3-P-18.1, International Travel Procedure for Mobile Devices, November 29, 2012.

12. CONTACTS

For further information, please contact your Information Security Officer. You also may contact the Office of Environmental Information, Office of Information Security & Privacy (OISP), Senior Agency Information Security Officer.

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: INTERNATIONAL TRAVEL PROCEDURE FOR MOBILE DEVICES PROCESS


Prior to Travel
Return From Travel
User
ISO
SAISO
OHS
Travel Approval
OITA Website
Start
1.0 Consult OITA Website on Travel Requirements
2.0 Contact ISO
12.0 Submit Equipment Request
End
Start
14.0 Return Equipment to Help Desk
End
Start
3.0 Coordinate on User Device Request
4.0 Submit Travel Info to SAISO
11.0 Inform User of Decision
End
Start
5.0 SAISO Review of Travel Request
6.0 Travel Destination Determination
10.0 Inform ISO of Decision
End
7.0 Submit Travel Info to OHS
Start
8.0 Review of Travel Request
9.0 Communicate Decision
SAISO
Who is Informed?
User
End
13.0 Inform User of Decision
End

APPENDIX B:
ACRONYMS & ABBREVIATIONS

BIOS	Basic Input/Output System
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
EPA	Environmental Protection Agency
FIAT	Fast International Approval and Tracking
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IMO	Information Management Officer
ISO	Information Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OEI	Office of Environmental Information
OHS	Office of Homeland Security
OISP	Office of Information Security & Privacy
OITA	Office of International and Tribal Affairs
OITO	Office of Information Technology Operations
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
SAISO	Senior Agency Information Security Officer
SD	Secure Digital
SIO	Senior Information Official
SSL	Secure Sockets Layer
USB	Universal Serial Bus
VPN	Virtual Private Network
WPA2	Wi-Fi Protected Access 2