While you're away:

- **Practice strong Operations Security (OPSEC).** Avoid the mention of sensitive topics, military movements, or other related activities. Limit discussions in public areas, hotel rooms, or other non-secure environments.
- **Maintain physical control of the device at all times.** Do not check the device with checked baggage at an airport, and do not secure the device in lockers or hotel safes.
- **Limit use of device.** Only use the device for official functions; the less you use the device, the less likely it will be compromised.
- **Remain alert of suspicious behaviors.**
- **Use encryption when possible.** Send encrypted e-mails, use approved VPN software, and utilize secure chat or voice means where possible.
- **Avoid solicitation attempts.** Do not discuss U.S. government related topics, and keep interactions with foreigners to a minimum. Do not exchange contact information.
- **Travel in a group.** Keeping a wingman with you will help you keep yourself and your equipment safe, identify suspicious events, and avoid dangerous interactions.

When you return:

- **Change your passwords.** Enable multi-factor authentication where available.

- **Review your web-based accounts for any suspicious activity.** Look over the messages that were sent from your account while you were traveling, review any devices that are authorized to access your account. Note any failed attempts to login to your account, if that information is available.

Report any suspicious incidents to AFOSI

AFOSI Confidential Web Tip Information System:
https://www.tip411.com/tips/new?alert_group_id=21111

AFOSI Home page:
http://www.osi.af.mil/

References:

- AFOSI. "Safeguarding USAF Personnel's Online Presence"
- "Industry Partners: Travel Tips - NCSC." Industry Partners: Travel Tips - NCSC. https://www.ncsc.gov/industry/travel/index.html
- "Turn On 2FA." Turn It On. https://www.turnon2fa.com

AFOSI

Traveling with Laptops and Mobile Devices

PROTECT YOURSELF

This handout provides simple security tips that DoD personnel can use to safeguard their electronic devices while traveling.

Traveling with Laptops and Mobile Devices

AFOSI

Threats to Travelers:

- **Criminals target DoD personnel and their belongings for theft or exploitation**. Criminals may resell stolen devices, or place malware on devices to access sensitive information, such as financial data.
- **Terrorists target DoD personnel for the purposes of kidnapping, causing physical harm, and/or exploitation.** A device may contain social media data which identifies other members of their family, unit, or professional organizations. Additionally, devices may contain other sensitive data, such as unit locations in mapping applications, photographs of unit members, and other sensitive information.
- **Foreign intelligence and security services (FISS) target DoD personnel and their belongings for theft, intimidation, exploitation, and as indicators of DoD activity.** FISS often place their officers at the airport and customs areas, to target DoD personnel and their devices during transit, security screenings, or customs interviews. In addition, FISS co-opt hotel staff for access into traveler's rooms and safes. FISS have the funding and expertise to employ technical exploitation (such as covert audio/video surveillance, network-based attacks, examination of fingerprints on a device to identify PIN codes, device tampering, and other advanced techniques.) FISS attempt to lure DoD members into situations involving alcohol, drugs, prostitution, and other illegal activity, in an attempt to solicit sensitive information, or blackmail DoD members.

Before Travel:

- **If you can do without the device, don't take it.** Don't take information you don't need, including sensitive contact information. Consider the consequences if your information were stolen by a foreign government or competitor.
- **Back up all information you take.** Leave the backed-up data at home.

- **Secure your social media, e-mail, and other Internet-based accounts.** Conduct a thorough review of all of your web-based accounts, and ensure that: your privacy settings are locked down appropriately; your secret questions, contact e-mail address or other security settings are up-to-date; you are using secure passwords; and consider the use of multi-factor authentication where available (keep in mind that you may not have your multi-factor device while traveling)
- **If feasible, use a different mobile phone**. Remove the battery when not in use. Ensure that your mobile device is also protected, in accordance with your agency guidelines and recommendations in this pamphlet.
- **Emergency Contacts**. You don't need an alpha roster, but you should always have basic contact information for your local U.S. Embassy, your base or organization, local police forces, and a POC in the U.S., in the event of an emergency while traveling.

Prepare your Device:

- **Create a strong password** (for laptops) or a long PIN # (mobile phones/tablets).

- **Enable device encryption.** If your device supports a "remote wipe" feature, learn how to use those functions.
- **Enable automatic locking of the device after a period of inactivity.**
- **Update your device's software and remove old or unused applications.** A device with outdated software can be easy to compromise by an attacker.
- **Disable unused hardware features.** Bluetooth, WiFi, GPS, NFC, and other features can likely be disabled, depending on your mission requirements.
- **Remove any unnecessary information from the device.** If this is an official device, consider having your agency "wipe" the device, and provide you with a "clean" software installation and software updates Ensure that your clean device is fully functional and up-to-date before travel.
- **Tell your device to keep a low profile: follow ATFP awareness training recommendations.** Agencies often require USG-owned devices to have property or inventory labels – but your device shouldn't scream "DoD TRAVELER" while in transit. Where appropriate, consider the use of civilian style bags, and device cases, as opposed to military-grade luggage to maintain a low profile.