Traveling with Portable Electronic Devices

YOU SHOULD KNOW

• In most countries you have no expectation of privacy in Internet cafes, hotels, offices, or public places. Hotel business centers and network connections are regularly monitored in many countries. In some countries, hotel rooms are often searched.

• All information you send electronically via your portable electronic device (PED) can be intercepted. Wireless devices are especially vulnerable.

• Foreign Intelligence Entities (FIEs) and criminals can track your movements using your PED and can turn on the microphone in your device even when you think it's off. To prevent this, remove the battery.

• FIEs and criminals can also insert malicious software on your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. When you connect to other networks or servers, the "malware" can migrate to your home, business, or agency, and can send information back to the malicious actor.

• If your device is equipped, malware can also be transferred through thumb drives and CD/DVD media.

• Transmitting controlled unclassified information and other sensitive government, personal, or proprietary information from abroad is risky.

• Government and corporate officials are most at risk, but don't assume you're too insignificant to be targeted.

• FIEs and criminals are adept at "phishing" – that is, pretending to be someone you trust in order to obtain sensitive information.

• If a customs official demands to examine your device, or if your hotel room is searched while the device is in the room and you're not, you should assume the device(s) is compromised.

BEFORE YOU TRAVEL

• If you can do without the PED, don't take it.

• Don't take information you don't need, including 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 work or home.

Traveling with Portable Electronic Devices

• If feasible, use a different PED, particularly mobile phone, from your usual one and remove the battery when not in use. In any case, have the device examined by your agency or company when you return.

PREPARE YOUR DEVICE

• Create a strong password (numbers, upper and lower case letters, special characters – at least 8 characters long). **Never store passwords, phone numbers, or sign-on sequences on any device or in its case.**

• Change passwords at regular intervals, and immediately upon your return.

• Use/Enable data-at-rest encryption on your PED.

• Download current and/or update antivirus protection, spyware protection, OS security patches, and a firewall before you travel.

• Encrypt all controlled unclassified and sensitive information on the PED. Note: In some countries, customs officials may not permit you to enter with encrypted data.

• Modify your web browser to higher, more strict security settings.

• Disable Wi-Fi, Bluetooth, and Location features; consider disabling applications you don't need while overseas.

WHILE YOU'RE AWAY

• Avoid transporting PEDs in checked baggage.

• Use digital signature and encryption when e-mailing controlled unclassified and other sensitive information; Use MS Office *protect* or *encrypt* capability for an e-mailed attachment.

• **Don't leave electronic devices unattended.** If you have to stow them, remove the battery and any removable drive or card (e.g. SIM chip, laptop hard drive, micro or mini SD card, etc.) and keep them with you.

• Shield passwords from view. Don't use the "remember me" feature on many websites; re-type the password every time.

• Be aware of who's looking at your screen, especially in public areas.

• Terminate connections when you're not using them; physically disable Wi-Fi and Bluetooth switch(es).

• After using any kiosk computer, clear the browser: delete history files, caches, cookies, URL, and temporary internet files.

Traveling with Portable Electronic Devices

• Don't open e-mails and/or attachments from unknown sources. Don't click on links in e-mails. Empty your "trash" and "recent" folders after every use.

• Avoid Wi-Fi and Bluetooth connections if you can. In some countries they're controlled by FIEs and **in all cases they place information at risk to collection and exploitation.**

• If your device or information is stolen, report it immediately to your organization and the local US embassy or consulate office.

WHEN YOU RETURN

• **Change your password.**

• Have your organization IT office examine the device for the presence of malicious software.

• For general travel alerts and information, see www.state.gov/travelandbusiness