DON Guidance for the Use of Electronic Devices During Travel

DON Guidance for the Use of Electronic Devices During Travel

DON personnel may be specifically targeted by adversaries due to the potential value of the information they possess or communicate. It is therefore essential that personnel take proactive steps to ensure the integrity and security of this information, and the integrity and security of the devices that process or store the information. This document provides guidelines to minimize the risk of compromising classified or sensitive information on electronic devices while on travel.

For the purposes of this guidance, electronic devices comprise all mobile computing and communications devices, including laptops, mobile phones, BlackBerrys and other smartphones, tablet devices such as the Apple iPad, and air cards. Connectivity may be provided via cellular, WiFi or, in the case of laptops, hard-wired to commercial networks such as in a home or hotel.

Traveling, particularly internationally, exposes mobile and wireless computing and communications devices to attack. These attacks include those that require physical access to the device, such as may be gained at an airport security checkpoint or hotel room, as well as indirect attacks that may be conducted over the air. In either case, the goal of the attack is to access the information on the device, without being detected by the user of the device.

While this document addresses government furnished equipment (GFE), many of these guidelines may be used to increase the security of your personal devices as well.

Common Vulnerabilities

Wireless Vulnerabilities

All wireless signals, such as cellular or WiFi, are susceptible to interception. Wireless devices also emanate radio waves, even when they are not actively being used. These characteristics make wireless devices a prime target. Awareness of the most popular means of wireless attacks will assist users in avoiding the most common pitfalls leading to compromised information.

Cellular Eavesdropping

Interception of voice or data transmissions may be accomplished with minimal investment and no engineering expertise – anybody can do it. Adversaries can also use cellular networks to remotely turn on the device and use it as a microphone. Thus, travelers may be unknowingly transporting a "bug" capable of hearing all within range of their device. In countries where the host nation operates or controls the cellular networks, these attacks may be state-sponsored and targeted towards specific individuals based on their rank or seniority.

Rogue Access Points

There are legitimate and illegitimate WiFi hot spots, and distinguishing the difference between the two can be difficult. WiFi devices continuously scan for and list all available networks. Rogue access points use naming conventions that appear legitimate, in order to attract users who are unaware of the authorized network name. Once connected to a rogue access point, all data transactions can be captured and copied, then passed on to its intended destination without any apparent impact on the user's session (called a man-in-the-middle attack).

Malicious Use of Location Services

Today, many wireless devices have the ability to provide location-based services – the ability to know, via Global Positioning System (GPS) or other means, the physical location of the device. This can be helpful for getting directions and finding restaurants. However, it also introduces the potential of a third party tracking the physical location of the device, and presumably, the user as well.

A lesser-known location-based vulnerability is the ability of some applications to automatically affix location data to documents or photos on the device, without the user's knowledge. This location data can be read by third parties interested in collecting behavioral information on their targets.

Wired Vulnerabilities

There are ways to compromise *wired* connections when on travel as well. Awareness of the most popular attacks on wired users will help travelers avoid compromising their information.

Poor Physical Security

Adversaries have been known to gain access to hotel wiring closets. As unencrypted information is passed, adversaries can easily monitor or launch attacks on both the data and voice connections to a traveler's room. Additionally, mobile computing and communication devices that are tethered to a wired connection are frequently left unattended for longer periods of time in order to maintain connection, making them susceptible to theft or tampering.

Malware and Keystroke Logging

Often travelers will use the hotel's business office computers, rather than their own. Business office systems may be set up to log every transaction or capture your key strokes. Additionally, malware can reside on these systems, attaching viruses or worms to files that are transferred between the business office systems and the traveler's system.

Do’s & Don’ts for Your Electronic Devices

The following guidelines describe actions that are easily executed and will significantly enhance the security posture of your electronic devices by mitigating the aforementioned threats. Additional travel guidance is available from the Defense Security Service (http://www.dss.mil). The Systems and Network Analysis Center at the National Security Agency (http://www.nsa.gov/snac) also maintains guidance on securing specific devices and technologies.

Avoid Cellular Eavesdropping

- Do not take your cell phone and other wireless devices into spaces where sensitive or classified information is stored or meetings are being held. If you must keep your device with you, turn it off and remove the battery.

  Why? *Cell phones, whether powered on or off, can be hacked and turned into a microphone without your knowledge. Powering off your cell phone is especially important during international travel where the host nation operates or controls the cellular networks.*

Avoid Rogue Access Points

- Do use WiFi Access Points provided by trusted sources. Take great care to verify the spelling of the network name prior to connection.

  Why? *A common attack on WiFi involves setting up false or rogue access points. Once a connection is made to these sites, hackers can initiate a man-in-the-middle attack, first capturing, then relaying all user transactions during the session.*

- Do not use unprotected transmissions while accessing the Internet from WiFi hot spots or networks, even if provided by trusted sources. When using WiFi to access the Internet from an NMCI computer, the system will automatically connect to the NMCI Virtual Private Network (VPN). Use of the VPN connection encrypts your activity, making it difficult to be monitored or compromised.

Wireless Off by Default

- Do not leave the wireless connection capability on, when no longer being used. Turn it off by default, and turn it on only when required.

  Why? *When on by default, the mobile and wireless computing and communication device continuously polls its surroundings, seeking out wireless access points and available networks in range for potential connection. Some connection points, particularly rogue access points, will accept a connection without challenge. Once connected, hackers can begin attacking your device without your knowledge.*

Avoid Malicious Use of Location Services

- Do not leave the GPS and other location service capabilities on, when they are no longer being used. Turn these capabilities off by default and turn them on only when required.

  Why? *The device, or the user carrying the device, can easily be tracked and targeted. Additionally, the continuous polling of the location service will cause the device’s battery to drain much faster than if used only when needed.*

Avoid Wired-Connection Vulnerabilities

- Do use GFE air cards whenever possible rather than unfamiliar wired network connections.

Enhance Physical Security

- Do not leave your computer or laptop unmonitored (particularly if powered on and unlocked).

  Why? *A computer or laptop left unmonitored and accessible, even if only for a few minutes, presents an opportunity for unauthorized access.*

- Do use the NMCI VPN connection while accessing the Internet from GFE via unfamiliar wired connections, even if checking your own personal mail. Use of the VPN connection encrypts your activity, making it difficult to be monitored or compromised. (Note: Accessing web-mail for limited personal use is now authorized on NMCI.)
- Do not leave your computer or laptop unattended and connected to the Internet for extended periods of time, while accessing unfamiliar wired connections.

  Why? *Occasionally, the NMCI VPN connection will drop due to low signal strength or time out due to inactivity. Hackers can easily monitor and copy all user transactions left open during the session; and with enough time, hackers may even be able to gain logical access to the device.*
- Do not leave your Common Access Card (CAC) unattended while in your electronic devices.

Avoid Malware and Keystroke Logging

- Do not use unfamiliar computer systems – use GFE.

  Why? *Computer systems may be set up to log every transaction or capture your key strokes via the keyboard. Additionally, malware can reside on these systems, attaching viruses or worms to files that are transferred between the business office systems and the traveler's system.*
- Do ensure anti-virus and anti-spyware applications are kept up to date and are actively running on your electronic devices. If you must transfer files from a hotel business office system to your mobile device, ensure you check it for viruses or spyware prior to accessing the files.

Other Mitigation Strategies

Inspect for Tampering

- Do frequently inspect your mobile and wireless computing and communications devices for signs of tampering. Tampering may include visible scratches or even abnormal behavior (e.g., sluggish).

  If tampering is evident, or even suspected, immediately remove the battery and/or SIM card. Then inform the command Information Assurance Manager as soon as practical.

Travel Light

- Do take only the bare minimum equipment you need to be productive. The fewer the number of devices you have, the fewer opportunities for compromise by an adversary.
- Do ensure you verify the power and outlet requirements for your destination. Newer electronic devices typically can accommodate the changes in voltage; however, older devices will need a transformer. Plug and cord adaptors are available to meet all of your traveling needs and should be considered, particularly if traveling abroad.
- Do not put mobile and wireless computing and communication devices in checked baggage.

  Why? *Unmonitored devices are at risk of being tampered with or having the contents copied.*

Use "Clean" Devices

- Do use loaner GFE mobile and wireless computing and communications devices whenever practical.

  Why? *Devices routinely used for work often contain more information than you will require on the trip. The use of designated devices for travel that are inspected and erased after each trip will minimize the impact of any compromise.*

Ensure Email Authentication

- Do digitally sign and encrypt your email whenever possible.
- Do not make a habit of using devices that are not CAC enabled.

  Why? *Transmissions from mobile and wireless computing and communications devices are extremely vulnerable to interception. Emails can appear to be sent from someone other than the actual sender (called spoofing). Signing and encrypting your emails will give the recipient a sense of security in knowing that the information you are sharing is authentic. Encrypting your emails will also prevent others from reading the contents, without specifically being authorized.*

Use Strong Passwords

- Do enable passcodes/passwords for all mobile and wireless computing and communications devices. Always use strong/complex passwords (i.e., those containing a combination of numbers, letters and special characters) where supported.
- Do not write down and attach passwords to the electronic devices.

Maintain Physical Control

- Do maintain positive control of all of your electronic devices.

  Why? *It takes mere seconds for an adversary to install tracking, bugging or other malicious software (malware) on a mobile electronic device. Secure devices when you cannot be with them (e.g., place in a room safe capable of being locked with your own personal locking device).*

Security Checkpoints

- Do take steps to ensure your device cannot be tampered with during security checkpoints.
- Remove the battery and/or SIM cards and keep them separate from the device.
- Do take steps to ensure classified-capable devices such as Secure Mobile Environment Portable Electronic Device (SME PED) are not activated during a security check. When possible, put the device in a clear, tamper-evident bag such as those provided by the National Security Agency.

  Why: *The device may be examined as necessary by security staff but cannot be physically tampered without ripping the bag open.*

Classification Levels

- Do not transmit, either through voice or data connection, information at a higher classification level than authorized for the device being used or your surroundings.
- Do pay close attention to the active operating mode when using multi-level security devices (e.g., SME PED).
- Do keep classification labels on mobile and wireless communication devices, particularly if you have similar devices that operate at different classification levels.

Limit Downloads to Authorized Activity

- Do not download executable files, unauthorized code or applications, including ring tones or MP3 files, to GFE mobile computing and communication devices.

  Why? *To protect against the inadvertent introduction of viruses and other malware into DoD networks, DoD policy prohibits such activity without express permission from the Designated Accrediting Authority (DAA).*

Bluetooth Use

- Do turn Bluetooth connectivity off when not in use. Set the default for the Bluetooth connection and the default for the device discovery (or visibility) off. Turn one or both capabilities on only when needed.
- Do not attempt to jail break and connect GFE mobile devices to unauthorized Bluetooth devices. The only approved use for Bluetooth wireless connectivity at this time is to support the Common Access Card reader. Bluetooth headsets and similar peripheral devices are not permitted.

  Why? *Adversaries may exploit Bluetooth connections, attaching to user devices without their knowledge and obtaining unimpeded access to the information stored or transmitted.*

Verify Coverage

- Do verify that the wireless carrier supported by your device provides adequate network coverage to your intended travel area prior to departure.

  Why? *DoD personnel have access to multiple mobile carrier service providers. If coverage is inadequate, ask that a device or air card be issued to you that will work at your destination. International service is also available for voice and data use, but must specifically be activated to ensure connection while traveling abroad and avoid excessive toll charges.*

USB Connection Use

- Do not connect mobile devices to unknown computers or devices, even to recharge your battery via the USB cable – bring your charger.

  Why? *Establishing a wired connection to your device provides a direct link for malicious activity.*

Use Devices with Data At Rest (DAR) Encryption

- Do ensure DAR encryption is installed and enabled on all mobile and wireless computing and communication devices, if available.

  Why? *Mobile and wireless computing and communication devices are easily stolen or lost. When DAR encryption is enabled with a strong password, it is nearly impossible for anyone to access the information on the device without the user's consent.*

Take This With You!

This handy reference card is designed for you to put in your pocket and take on your next trip.

Do's & Dont's Quick Reference Guide

DO NOT take your cell phone and other wireless devices into spaces where sensitive or classified information is stored or meetings are being held. If you must keep your device with you, turn it off and remove the battery.

DO use WiFi Access Points provided by trusted sources. Take great care to verify the spelling of the network name prior to connection.

DO NOT use unprotected transmissions while accessing the Internet from wired or wireless networks, even if provided by trusted sources. Always use the NMCI Virtual Private Network (VPN) connection while accessing the Internet.

DO NOT leave the wireless connection capability on, when no longer being used. Turn it off by default, and turn it on only when required.

DO NOT leave the GPS and other location service capabilities on, when no longer being used. Turn these capabilities off by default and turn them on only when required.

DO use GFE air cards whenever possible rather than unfamiliar wired network connections.

DO NOT lose positive control of your electronic device (particularly if powered on and unlocked).

DO use the NMCI VPN to access your personal mail while on travel. Accessing web-mail for limited personal use is now authorized on NMCI.

DO NOT leave your computer or laptop unattended and connected to the Internet for extended periods of time, while accessing unfamiliar wired or wireless connections.

DO NOT leave your Common Access Card (CAC) unattended while in your electronic devices.

DO NOT use unfamiliar business office systems – use GFE.

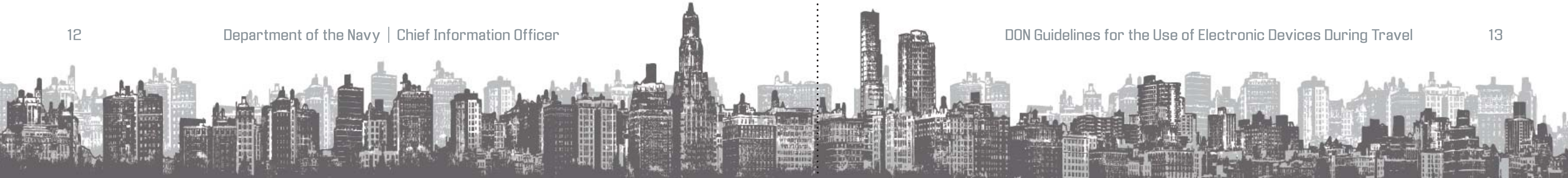
DO ensure anti-virus and anti-spyware applications are kept up to date and are actively running on your electronic devices. If you must transfer files from a business office system to your mobile device, ensure you check it for viruses or spyware prior to accessing the files.

DO NOT make a habit of using devices that are not CAC enabled.

DO digitally sign and encrypt your email whenever possible.

DO frequently inspect your mobile and wireless computing and communications devices for signs of tampering. Tampering may include visible scratches or even abnormal behavior (e.g., sluggish). If tampering is evident, or even suspected, immediately remove the battery and/or SIM card. Then inform the command Information Assurance Manager as soon as practical.

DO take only the bare minimum equipment you need to be productive while on travel.



DO ensure you verify the power and outlet requirements for your destination. Newer electronic devices typically can accommodate the changes in voltage; however, older devices will need a transformer. Plug and chord adaptors are available to meet all of your traveling needs and should be considered, particularly if traveling abroad.

DO NOT put mobile and wireless computing and communication devices in checked baggage.

DO use “clean” loaner GFE mobile and wireless computing and communications devices whenever practical.

DO ensure DAR encryption is installed and enabled on all mobile and wireless computing and communication devices, if available.

DO take steps to ensure your device cannot be tampered with during security checkpoints. Remove the battery and/or SIM cards and keep them separate from the device.

DO take steps to ensure classified-capable devices such as SME PEDs are not activated during a security check. When possible, put the device in a clear, tamper-evident bag such as those provided by the NSA.

DO NOT transmit, either through voice or data connection, information at a higher classification level than authorized for the device being used or your surroundings.

DO pay close attention to the active operating mode when using multi-level security devices (e.g., the Secure Mobile Environment Portable Electronic Device (SME PED)).

DO keep classification labels on mobile and wireless communication devices, particularly if you have similar devices that operate at different classification levels.

DO report lost or stolen devices immediately.

DO enable passcodes/passwords for all mobile and wireless computing and communications devices. Always use strong/complex passwords (i.e., those containing a combination of numbers, letters and special characters) where supported.

DO NOT write down and attach passwords to the electronic devices.

DO NOT download executable files, unauthorized code or applications, including ring tones or MP3 files, to GFE mobile computing and communication devices.

DO turn Bluetooth connectivity off when not in use. Set the default for the Bluetooth connection and the default for the device discovery (or visibility) off. Turn one or both capabilities on only when needed.

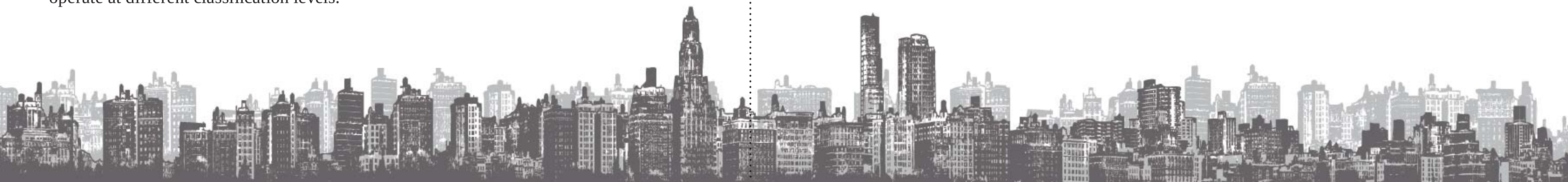
DO NOT attempt to jail break and connect GFE mobile devices to unauthorized Bluetooth devices. The only approved use for Bluetooth wireless connectivity at this time is to support the Common Access Card reader.

DO verify that the wireless carrier supported by your device provides adequate network coverage to your intended travel area prior to departure. If coverage is inadequate, request a substitute. International coverage is also available upon request.

DO NOT connect mobile devices to unknown computers or devices, even to recharge your battery via the USB cable – bring your charger.

MAINTAIN VIGILANCE!

It’s your ultimate responsibility to protect the information and devices which have been entrusted to you. Always assume you will be targeted, particularly when traveling abroad.



Department of the Navy
Chief Information Officer
Version 2.0 | March 2011