# Removable Media and Mobile Devices

## Removable Media, PEDs, and Mobile Devices

Removable media include flash media, such as thumb drives, memory sticks, and flash drives; external hard drives; optical discs (such as CDs, DVDs, and Blu-rays); and music players (such as iPods). Other portable electronic devices (PEDs) and mobile computing devices, such as laptops, fitness bands, tablets, smartphones, electronic readers, and Bluetooth devices, have similar features. The same rules and protections apply to both.

## Risks Associated with Removable Media

The risks associated with removable media include:

- Introduction of malicious code
- Compromise of systems' confidentiality, availability, and/or integrity
- Spillage of classified information

Potential consequences:

- Shutdown of systems
- Compromise of information, systems, programs, and/or assets
- Loss of mission
- Loss of life

## Approved and Prohibited Devices

Your organization may severely restrict or prohibit the use of removable media and PEDs. Follow your organization's policies or contact your security POC with questions.

- Use only removable media approved by your organization
- Only use flash media or other removable storage when operationally necessary, owned by your organization, and approved by the appropriate authority in accordance with policy
- Do not use any personally owned/non-organizational removable media on your organization's systems
- Do not use your organization's removable media on non-organizational/personal systems
- Never plug unauthorized devices into a government system
- Be aware that wireless connections to the devices bring increased threats and vulnerabilities
- Abide by the signed End User License Agreement for mobile devices
- Understand and follow your organization's approved mobile device policy

## Appropriate Use of Removable Media

If your organization allows it, use removable media and PEDs appropriately:

- Do not download data from the classified networks onto removable storage media

- Encrypt data appropriately and in accordance with its classification or sensitivity level
- As a best practice, label all removable media regardless of classification or environment and avoid inserting removable media with unknown content into your computer
- Store according to the appropriate security classification in GSA-approved storage containers
- Mark all classified and sensitive material correctly
- Ensure unclassified media in a classified environment is labeled appropriately
- Label all media containing Privacy Act information, personally identifiable information (PII), or protected health information (PHI) appropriately regardless of environment
- Follow your organization's policy for sanitizing, purging, discarding, and destroying removable media
- Destroy classified removable media in accordance with its classification level

## SCIFs and Removable Media

When using removable media in a SCIF:

- Users must properly identify and disclose removable media with local Configuration/Change Management (CM) Control and Property Management authorities
- Users shall comply with site CM policies and procedures
- Media shall display a label inclusive of maximum classification, date of creation, POC, and CM Control Number

## Protecting Data on Mobile Devices and PEDs

To protect data on your mobile computing and portable electronic devices (PEDs):

- Lock your laptop/device screen when not in use and power off the device if you don't plan to resume use in the immediate future
- Enable automatic screen locking after a period of inactivity
- Encrypt all sensitive data on laptops and on other mobile computing devices when possible
- At a minimum, password protect Government-issued mobile computing devices; use two-factor authentication if possible
- Secure your personal mobile devices to the same level as Government-issued systems
- Understand your organization's policy for using commercial cloud applications (e.g., Dropbox, Drive, etc.)
- Maintain visual or physical control of your laptop and mobile devices at all times and especially when going through airport security checkpoints
- Have a strategy for addressing a potential "authority situation" (e.g., police who want to inspect devices coincident with a traffic stop or an airport TSA agent check)
- If lost or stolen, immediately report the loss to your security POC

## Traveling with Mobile Devices

When traveling with mobile computing devices, including laptops and cell phones:

- Be aware that information sent over public Wi-Fi connections may be exposed to theft, and the device may be exposed to malware
- Fake Wi-Fi access points may be used for deception
- Use public or free Wi-Fi only with the Government VPN

Use caution when connecting laptops to hotel Internet connections. If you are directed to a login page before you can connect by VPN, the risk of malware loading or data compromise is substantially increased.

When traveling overseas with mobile devices:

- Assume that any electronic transmission you make (voice or data) may be monitored
  - Mobile phones carried overseas are often compromised upon exiting the plane
- Physical security of mobile devices carried overseas is a major issue
- Devices not in your custody or in secure U.S. Government facility storage should be assumed to be compromised

## Public Use of Mobile Devices

When using mobile computing devices, including laptops and cell phones, in public:

- Be careful of information visible on your mobile computing device; consider screen protection
- Maintain possession of laptop and other government-furnished equipment (GFE) at all times and be extra vigilant in protecting it
- Protect your mobile computing device using a password or other access control (i.e., two-factor authentication)
- Make certain all sensitive data stored on your laptop is encrypted
- Avoid using Government computers in non-secure environments
  - DoD employees are prohibited from using a DoD CAC in card-reader-enabled public devices such as those found in public libraries and Internet cafes
- Never discuss sensitive information in public, even if using a secure device

## Near Field Communication (NFC)

Exercise caution when using near field communication (NFC):

- NFC is wireless technology that enables your electronic devices to establish communications and exchange information when placed next to each other. Smartphones can be enabled to:
  - Read electronic tag information, such as proximity cards or other objects with embedded NFC tags
  - Transmit information electronically, such as when making credit card payments with information held on the smartphone
- Security risks:
  - Eavesdropping: an adversary intercepts the signal
  - Data manipulation or corruption: an adversary intercepts the signal and alters it

    - Viruses: stored financial or mission information increases potential rewards for hackers
- Only use NFC with your Government-furnished device as instructed and permitted by your organization

## GPS on Mobile Devices

Many mobile devices and applications can track your location without your knowledge or consent. Mobile device tracking can:

- Geolocate you
- Display your location
- Record location history
- Activate by default

Stop and think before you wear or use a mobile device!

## AMD Programs

When participating in an approved mobile device (AMD) program:

- Read and sign the User Agreement that includes the program's requirements and policies
- Use of your personal device depends on your organization's policies
- The approved device will be provisioned to employ necessary security measures to secure it and its data when accessed