

## Cyber Awareness Challenge Reference Material

# Mobile Computing and Removable Media

---

### Portable electronic devices (PEDs) include—

- Laptop computers
- Cell phones and smartphones
- Wireless readers (such as Kindles and iPads)
- Tablet computers

### Removable media include:

- Thumb drives, memory sticks, flash drives
- CDs and DVDs
- External hard drives
- Music players (such as iPods)

### Tips for Security of Mobile Computing & PEDs

- Lock your laptop or device screen when not in use
- Encrypt all sensitive data on laptops and on other mobile computing devices when possible
- Password protect government-issued mobile computing devices
- Maintain visual or physical control of your laptops and mobile devices at all times and especially when going through airport security checkpoints
- If lost or stolen, immediately report the loss to your security POC

### Tips for Use of Wireless Technology

Wireless technology includes Bluetooth, infrared, and wireless computer peripherals (that is, wireless keyboard, wireless mouse, and so on).

### To protect information systems and data on those systems:

- Be cautious when using wireless technology:
  - Ensure that the wireless security features are properly configured
  - Turn off or disable wireless capability when connected via LAN cable
  - Turn off or disable wireless capability when not in use
  - Avoid using non-Bluetooth paired or unencrypted wireless peripherals (that is keyboard, mouse, and so on)
- Follow your organization's policies for proper configuration of wireless security features

**Remember!** Wireless technology is inherently not a secure technology.

## Tips for Removable Media Use

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

### Use appropriately, if allowed at all:

- Do not use flash media unless operationally necessary, owned by your organization, and approved by the appropriate authority in accordance with policy
- Do not use any personally owned or non-organization removable flash media on your organization's systems
- Do not use your organization's removable flash media on non-organization or personal systems
- Use only removable media approved by your organization
- Do not download data from the classified networks onto removable storage media
- Encrypt data appropriately and in accordance with its classification or sensitivity level

## Tips for Protecting Removable Media

### To protect removable media:

- Store according to the appropriate security classification in GSA-approved storage containers
- Label all classified and sensitive material correctly
- Ensure unclassified media in a classified environment is labeled appropriately
- Label all media containing Privacy Act information, PII, or 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
- As a best practice, label all removable media regardless of classification or environment and avoid inserting removable media with unknown content into your computer.

## Tips for Travelling

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

- Be careful of information visible on your mobile computing device
- Maintain possession of laptop and other government-furnished equipment (GFE) at all times and be extra vigilant in protecting it
- Password protect your mobile computing device
- 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
- Do not use your CAC/PIV on systems without updated system security protections and anti-virus
- Never discuss sensitive information on an unsecure phone

- 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.