Telework and Home Computer Security

Telework

To telework, you must:

- Have permission from your organization
- Follow your organization's guidance to telework
- Use authorized equipment and software and follow your organization's policies
- Employ cybersecurity best practices at all times, including when using a Virtual Private Network (VPN)
- Perform telework in a dedicated area when at home
- Position your monitor so that it is not facing windows or easily observed by others when in use

Do not remove classified documents from your secure workspace to work offsite! Classified documents, either in hard copy or electronic format, are strictly prohibited. Be sure to safeguard all DoD data while teleworking.

Peripherals

Follow policy for using personally-owned computer peripherals with government furnished equipment (GFE):

- Permitted
  - Monitors, with the following conditions:
    - Connected via Visual Graphic Array (VGA), Digital Video Interface (DVI), High-Definition Multimedia Interface (HDMI), or DisplayPort
    - No other devices connected to the monitor
  - Wired keyboards, mice, and trackballs through a Universal Serial Bus (USB) connection
  - USB hubs
  - Headphones and headsets, with or without microphones, through a USB port
- Not permitted
  - Monitors connected via USB
  - Peripherals manufactured by any prohibited source (refer to the course Resources)
  - Bluetooth and other wireless external computer peripherals
  - Installation of drivers to support personally-owned peripherals

Wireless Network

When using a home wireless network for telework:

- Implement Wi-Fi Protected Access 2 (WPA2) Personal (also known as WPA2 Pre-Shared Key) encryption at a minimum on your wireless router
- Limit access to your wireless network and allow access only to specific devices

- Change the Service Set Identifier (SSID) of your router from the default and your router's pre-set password using a strong password
- Immediately establish a virtual private network (VPN) after connecting

Wireless Technology

Wireless technology includes Bluetooth, infrared, wireless computer peripherals (e.g., wireless keyboard, wireless mouse, etc.), and smart devices (e.g., smart refrigerators, medical pumps, wireless-enabled hearing aids).

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/disable wireless capability when connected via LAN cable
- Turn off/disable wireless capability when not in use
- Avoid using non-Bluetooth paired or unencrypted wireless peripherals (e.g., keyboard, mouse, etc.)
- Follow your organization's policies for proper configuration of wireless security features

Remember! Wireless technology is an inherently insecure technology.

Internet of Things (IoT)

Smart devices in your home, such as voice-enabled devices, enhanced remotes, smart thermostats, security cameras, smart speakers, smart televisions, doorbell cameras, smart thermostats, smart watches, smart appliances, smart tags, other programmable appliances, and even automobiles are part of what is known as the Internet of Things (IoT). The "things" within the IoT rely on a connection to the cloud, sometimes using another device as a relay, to analyze and act on the data they gather. For example, consider a smart lightbulb. You may use an app on your smartphone, tablet, or a voice activated digital assistant accessed through another device, such as a smart speaker, television, or watch, to operate it.

IoT devices can be compromised within two minutes of connecting to the Internet, and default passwords are currently the biggest security weaknesses of these devices. When using your home network to telework, an unsecured IoT device could become an attack vector to any attached government-furnished equipment (GFE). To secure IoT devices:

- Examine the default security options available and enable any security features
    - Remove or turn off voice-enabled listening and recording devices in your telework environment
    - Disable voice to text functions on Intelligent Personal Virtual Assistant Applications (IPVA) residing on any of your mobile or networked devices when teleworking
    - Most IPVAs, when enabled, are always listening for sounds or commands, which includes background conversations

    - Deny IPVAs access permission to any data that you consider risky or do not want to share
- Set a robust password at the device's maximum length, if possible
- Check your device's Bluetooth connections periodically to ensure that there are no unknown devices connected

For each device, check the user manual or go to the manufacturer's website to learn more about its data collection policies and how to enable security features and disable audio and recording functions. Regularly monitor the device manufacturer's website for firmware updates and ensure updates are installed when available.

Best Practices for Home Computer Security

Defend yourself! Keep your identity secure/prevent identity theft.

When working at home on your computer, follow these best security practices, derived from the National Security Agency (NSA) datasheet "Best Practices for Keeping Your Home Network Secure."

- Turn on password feature, create separate accounts for each user, and have them create their own passwords using a strong password creation method
- Install all system security updates, patches, and keep your defenses up-to-date
- Keep antivirus software up-to-date
- Regularly scan files for viruses
- Install spyware protection software
- Turn on firewall protection
- Require confirmation before installing mobile code
- Change default logon ID and passwords for operating system and applications
- Regularly back up and securely store your files

Antivirus Software

Some agencies may have discounted/free antivirus software available to their employees.

- Active DoD military and civilian employees may install antivirus software for personal device protection via the DoD Antivirus Home Use Program