Identity Authentication

For identity authentication, the Department of Defense (DoD) is moving toward using two-factor authentication wherever possible. Two-factor authentication combines two out of the three types of credentials to verify your identity and keep it more secure:

- Something you possess, such as a Common Access Card (CAC)
- Something you know, such as your Personal Identification Number (PIN)
- Something you are, such as a fingerprint or other biometrics

Use two-factor authentication wherever possible, even for personal accounts. For example, some widely used personal services (like Google) offer two-factor authentication.

Passwords

When using passwords at work or at home, create strong passwords:

- Combine letters, numbers, and special characters
- Do not use personal information
- Do not use common phrases or dictionary words in any language
- Do not write down your password; memorize it
- Follow your organization’s policy on:
  - Password length
  - Frequency of changing your password: best practice is at least every 3 months
- Avoid using the same password between systems or applications

CAC/PIV Card

The Common Access Card (CAC)/Personal Identity Verification (PIV) card is a controlled item. It implements DoD Public Key Infrastructure (PKI) and contains certificates for:

- Identification
- Encryption
- Digital signature

Note: Some systems use different types of smart card security tokens. Avoid a potential security violation by using the appropriate token for each system.
Cyber Awareness Challenge 2022

Computer Use

CAC/PIV Card Protection

To protect your CAC/PIV card:

- Maintain possession of your CAC/PIV card at all times
  - Remove and take your CAC/PIV card whenever you leave your work station
  - Never surrender or exchange your CAC/PIV card for building access (e.g., a visitor pass)
  - If your CAC/PIV card is lost or misplaced, report it immediately to your security POC
- Store it in a shielded sleeve to mitigate card and chip cloning
- Do not write down or share the PIN for your CAC/PIV card
- Avoid using your CAC/PIV card as a form of photo identification when there is a request for such verification by a commercial entity
- Do not allow commercial entities to photocopy or duplicate your CAC/PIV card
- Lock your computer when you leave or shut it down, depending on your organization’s security policy
- Do not use your CAC/PIV card on systems without updated system security protections and antivirus
- Use all security tokens appropriately

DoD PKI Tokens

When using a DoD PKI token:

- Only leave in a system while actively using it for a PKI-required task
- Never use on a publicly accessible computer (e.g., kiosks, internet cafes, and public libraries)
- Never use on a computer with out-of-date antivirus software or without spyware and malware protection
- Only use a token within its designated classification level
  - Never use a token approved for NIPRNet on a system of a higher classification level
  - Never use a token for a higher classification system on a system of a lower classification level (e.g., do not use a SIPRNet token on the NIPRNet)
  - Know and comply with the security requirements for tokens for higher classification systems
- If misuse occurs, report it immediately to your security POC

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 inherently not a secure technology.

**Internet of Things**

Smart devices in your home, such as voice-enabled devices, enhanced remotes, smart thermostats, security cameras, and other programmable appliances, are part of what is known as the Internet of Things (IoT). IoT devices can be compromised within two minutes of connecting to the Internet, and default passwords are currently the biggest security weakness 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
- Enable any security features
- Set a robust password at the device’s maximum length, if possible

**Cookies and Website Use**

A cookie is a text file that a web server stores on your hard drive. Cookies may pose a security threat, particularly when they save unencrypted personal information. Cookies also may track your activities on the web.

To prevent cookies from being saved to your hard drive:

- If you have the option, set your browser preferences to prompt you each time a website wants to store a cookie
- Only accept cookies from reputable, trusted websites
- Confirm that the site uses an encrypted link
  - Look for “h-t-t-p-s” in the URL name
  - Look for an icon to indicate the encryption is functioning
- Be especially aware of cookies when visiting e-commerce sites or other sites that may ask for credit card or other personal information

Note: Not all https sites are legitimate and there is still a risk to entering your information online.
Identity Protection

To protect your identity:

- Ask how information will be used before giving it out
- Pay attention to credit card and bank statements
- Avoid common names/dates for passwords and PINs
- Never share passwords and PINs
- Pick up mail promptly
- Do not leave outgoing postal mail in personal or organizational mailboxes, unless secured with a locking mechanism
- Shred personal documents
- Refrain from carrying SSN card and passport
- Order credit report annually

To respond to identity theft if it occurs:

- Contact credit reporting agencies
- Contact financial institutions to cancel accounts
- Monitor credit card statements for unauthorized purchases
- Report the crime to local law enforcement