

## Cyber Awareness Challenge Reference Material

# Network Access Security

---

### Physical Security

Physical security protects the facility and the information systems or infrastructure, both inside and outside the building.

#### To practice good physical security:

- Know and follow your organization's policy on:
  - Gaining entry
  - Securing work area
  - Responding to emergencies
- Use your own security badge or key code
  - Note that your CAC/PIV is sometimes used as an access badge
- Don't allow others access or to piggyback into secure areas
- Challenge people without proper badges
- Report suspicious activity

### Password Security

Each organization has its own policy on passwords, but there are some general guidelines you should follow to protect government information systems from being compromised.

Use these guidelines when creating passwords at home to keep your home computer secure as well. Remember to use different passwords for work and for home.

#### Tips for Creating Strong Passwords

- Combine letters, numbers, special characters
- Do not use personal information
- Do not use common phrases or words
- Do not write down your password; memorize it
- Follow your organization's policy on—
  - Password length
  - Changing your password

## Tips for Protecting Your CAC/PIV or Security Token

A Common Access Card (CAC)/Personal Identity Verification (PIV) is a controlled item that implements DoD Public Key Infrastructure (PKI).

### A CAC/PIV contains certificates for:

- Identification
- Encryption
- Digital signatures

**NOTE:** Some systems use different types of security tokens. Be sure to use the appropriate token for each system.

### To protect your CAC/PIV:

- Use all security tokens appropriately
- Remove and take your CAC/PIV whenever you leave your workstation
- Lock your computer when leaving, and shut it down at the end of your shift
- Do not use your CAC/PIV for badge exchanges
- Do not write down or share your personal identification number (PIN) for your CAC/PIV
- Maintain possession of your CAC/PIV at all times
- If your CAC/PIV is lost or misplaced, report it immediately to your security POC

## DoD Public Key Infrastructure (PKI) Token

### Special requirements for DOD Public Key Infrastructure (PKI) tokens:

- Only leave in a system while actively using it for a PKI-required task
- Never use on a publicly accessible computer (such as kiosks, Internet cafés, and public libraries)
- Never use on a computer with out-of-date anti-virus software or spyware and malware protection
- Always use within designated classification level
  - Never use tokens approved for NIPRNet use on systems of a higher classification level
  - Never use tokens for a higher classification system on systems of a lower classification level (for example, do not use SIPRNet tokens on the NIPRNet)
- If misuse occurs, report it immediately to your security POC