Government Facilities and Resources

Physical Security

Physical security protects the facility and the information systems/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/key code. Note that your Common Access Card (CAC)/Personal Identity Verification (PIV) card is sometimes used as a facility access badge.
- Don't allow others access or to piggyback into secure areas
- Challenge people without proper badges
- Report suspicious activity
- Protect access rosters from public view (e.g., do not take them home or post them in public spaces, such as bulletin boards)

Situational Awareness

To avoid being targeted by adversaries, remain aware of your surroundings. For example:

- Remove your security badge after leaving your controlled area or office building
- Don't talk about work outside your workspace unless it is a specifically designated public meeting environment and is controlled by the event planners
- Even inside a closed work environment, be careful when discussing classified or sensitive information, such as PII or PHI, as people without a need-to-know may be present
- Avoid activities that may compromise situational awareness
- Be aware of people eavesdropping when retrieving messages from smartphones or other media

Collateral Classified Spaces

Follow your organization's policy on mobile devices and peripherals within secure spaces where classified information is processed, handled, or discussed. Mobile devices and peripherals may be hacked or infected with malware and can be used to track, record, photograph, or videotape the environment around them. Powering off or putting devices in airplane mode is not sufficient to mitigate these risks and the threat these devices pose to classified information.

When using unclassified laptops and peripherals in a collateral classified environment:

- Ensure that any embedded cameras, microphones, and Wi-Fi are physically disabled
- Use authorized external peripherals only
  - Government-issued wired headsets and microphones

- Government-issued wired webcams in designated areas
- Personally-owned wired headsets without a microphone

All wireless headsets, microphones, and webcams are prohibited in DoD classified spaces, as well as all personally-owned external peripherals other than wired headsets.

Sensitive Compartmented Information Facilities (SCIFs)

Within a Sensitive Compartmented Information Facility (SCIF):

- Everyone must badge in – no piggybacking
- Personnel entering or leaving an area are required to secure the entrance or exit point
- Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's need-to-know and access
- Badges must be visible and displayed above the waist at all times while in the facility
- Badges must be removed when leaving the facility

If an incident occurs in a SCIF:

- Notify your security POC about the incident
- An analysis of the media must be conducted for viruses or malicious code
- The other workstations in the SCIF must also be analyzed
- If the incident was unintentional, then the person may have to attend a refresher training course in security awareness

SCIF Situational Awareness

Situational awareness and SCI:

- Do not discuss sensitive or classified information around non-cleared personnel, personnel without a need-to-know, or outside of a properly secured facility, as it could lead to a compromise of SCI.
- When discussing sensitive or classified information, physically assess that all personnel present or within listening distance have a need-to-know for the information being discussed
- Do not hold phone conversations on unencrypted phones in the vicinity in which classified or sensitive information is being discussed
- Ensure monitors do not provide unobstructed views of classified information – monitors facing windows should be turned or the window blinds should be closed
- Ensure uncleared persons are escorted by a cleared person familiar with the facility security procedures
- Warn those in the SCIF that uncleared personnel are present in the secure facility or working area

When sharing information in a SCIF:

- Follow security practices for protecting classified material; do not assume open storage just because you are in a SCIF

- Ensure that the person with whom you are sharing information is properly cleared and has a need-to-know
- Do not reference or hyperlink derivatively classified reports, documents, records, or articles that are classified higher than the audience in receipt
- Do not share any information with any individuals without checking need-to-know
- Balance the need to share intelligence with the need to protect sources and methods
- Appropriately mark and protect all classified material

SCIFs and Portable Electronic Devices (PEDs)

No personal PEDs are allowed in a Sensitive Compartmented Information Facility (SCIF). Government-owned PEDs must be expressly authorized by your agency. When using a government-owned PED:

- Only connect government-owned PEDs to the same level classification information system when authorized
- Only use devices of equal or greater classification than the information you are accessing or transmitting
- Ensure secure device is properly configured and updated
- Don't discuss classified information over smartphones
- Don't view classified information via device when not in a cleared space

As a general rule, there should be no Wi-Fi, Bluetooth, cellular, image capturing, video recording, or audio recording capabilities or wearable devices in the SCIF. Check with your security officer or your agency's policies.

Cyberspace Protection Conditions (CPCON)

The United States Cyber Command (USCYBERCOM) Instruction 5200-13 establishes Cyberspace Protection Conditions (CPCON) for the DoD. CPCON establishes protection priorities for each level during significant cyberspace events, as shown in the table below. Depending on the CPCON level, users may experience disruptions in service or access to physical spaces.

CPCON Level	DoD Risk Level	Priority Focus
CPCON 1	Very High	Critical Functions
CPCON 2	High	Critical and Essential Functions
CPCON 3	Medium	Critical, Essential, and Support Functions
CPCON 4	Low	All Functions
CPCON 5	Very Low	All Functions

Zero Trust

DoD is adopting a Zero Trust (ZT) model of cybersecurity that focuses on protecting data within modern computing environments, including cloud-based data and worldwide remote access. Unlike traditional cybersecurity that focuses on protecting a network perimeter, the ZT framework assumes that a breach has already happened or is going to happen. It limits

access to data, applications, assets, and services on a need-to-know basis, meaning that every user and device must continuously prove their trustworthiness. As ZT implementation proceeds, you can expect to experience:

- More restrictive access controls. Users are only given access to the resources they absolutely need to limit the potential impact of a security breach.
- Improved data protection. Critical data is identified and protected as the priority.
- Continuous monitoring to allow quicker detection and response to potential threats.
- More frequent security verification to authenticate and authorize every user, device, and application.
- Enhanced security posture. By assuming no user or device can be trusted by default, ZT greatly reduces the risk of lateral movement and data breaches.

Ethical Use of Government-Furnished Equipment (GFE)

Ethical use of government furnished equipment (GFE):

- Use GFE for official purposes only
- Don't allow unauthorized users to use your GFE
- Don't view or download pornography
- Don't gamble on the Internet
- Don't conduct private business/money-making ventures
- Don't load or use personal/unauthorized software or services, such as DropBox or peer-to-peer (P2P) software
    - P2P software can compromise network configurations, spread viruses and spyware, and allow unauthorized access to data
- Only use streaming video and audio for official business and in accordance with your organization's policy
- Don't illegally download copyrighted programs or material
- Don't make unauthorized configuration changes
- Only check personal e-mail if your organization allows it
- Don't play games unless allowed by your organization to do so on personal time
- Always physically secure your device, including when working from home

Note: All DoD-owned devices are subject to monitoring. When you use these devices, you authorize the monitoring of your activity on these devices.

Use of Government E-mail

E-mail use must not adversely affect performance of your role or reflect poorly on your organization. To use e-mail appropriately:

- Do not use e-mail to sell anything
- Do not send:
    - Chain letters
    - Offensive letters
    - Mass e-mails
    - Jokes
    - Unnecessary pictures

    - Inspirational stories
- Avoid using "Reply All" to prevent sending unnecessary e-mail traffic
- Only use e-mail for personal reasons if allowed by your organization
- Use a digital signature when sending attachments or hyperlinks, as required by the DoD
- Do not use personal accounts, such as webmail, to conduct official DoD communication

Use of Other Tools for Government Purpose

Follow DoD and your organization's policy on the use of any technology with Government data, including:

- Microsoft Teams and other non-email communication platforms
    - Communications in any format, including chats and SMS messaging, may be official records.
    - Before deleting any communication from a Government device, consider whether it is an official record.
- Webmail
    - Webmail is a web-based service that checks e-mail remotely.
    - If permitted, use webmail with caution as it may bypass built-in security features and other safeguards such as encryption.
- Adaptive artificial intelligence (AI)
    - The DoD Chief Digital and Artificial Intelligence Office (CDAO) leads and oversees the DoD's strategy and policy for AI digital services.
    - Ensure you only use adaptive AI tools approved by your organization on Government devices.
    - Exercise caution using adaptive AI tools on your personal devices.

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.

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 workstation
  - 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 operating system, applications, or 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