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

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