Center for Development of Security Excellence

CDSE

Learn. Perform. Protect.

Job Aid: Counterintelligence Awareness for Defense Critical Infrastructure

What Is CIP?

Critical Infrastructure Protection (CIP) is a national program to protect physical or virtual systems and assets so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, safety, or psychology, or any combination of these. CIP consists of actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets.

Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, or various other countermeasures. Federal departments and agencies have created CIP plans for protecting specific physical and cyber critical infrastructure key resources (CI/KR).

What Is DCIP?

The Department of Defense (DoD) implements its CIP through the **Defense Critical Infrastructure Program (DCIP)**. The goal of the DCIP is to coordinate the identification, assessment, assurance/protection and real time monitoring of physical and cyber infrastructures essential to the execution of the National Military Strategy.

How Does CI Support DCIP?

CI supports the DCIP by providing threat information, assessing risks, and developing countermeasures. Work with your CI office to determine the relationship between criticality, vulnerability, and threats. **Reporting** suspicious activity to your CI office will help to detect, deter, and neutralize the threat while mitigating associated risks. Access these **Resources** to learn more.

Threats to the DCIP Sectors

Threats to DCIP sectors are manifold and include foreign intelligence entities, commercial competitors, foreign and domestic terrorists, saboteurs, activists, hacktivists, hackers, organized criminal groups, individual actors, and trusted insiders. These actors vary considerably in terms of motivation and capability, but all incidents, regardless of the original motive, have the potential to disrupt critical systems, even inadvertently. Although the risk to critical infrastructure includes impact from weather-related disasters and other natural causes, this job aid focuses on the threat from human sources.

DCIP Sectors

Select each DCIP sector to see the risks and reportable suspicious activity associated with each sector.

- Defense Industrial Base (DIB)
- DoD Information Network (DoDIN)
- Financial Services
- Health Affairs
- Intelligence
- Logistics
- Personnel
- Public Works
- Space
- Transportation

Defense Industrial Base (DIB)

- **Know:** This sector includes cleared industry supporting the DoD mission capability, loss of which places the national defense at risk. The development of U.S. Defense technology and dual use technology make this sector a strong target for adversaries who may try to gain unauthorized access to classified or sensitive information.
- **Be alert for:** Attempts to illegally acquire U.S. defense technology, the exploitation of foreign visits, and unusual requests for information.

DoD Information Network (DoDIN)

- **Know:** The DoDIN (formerly Global Information Grid, GIG) is an information systems functions-based sector comprising physical assets and virtual systems and networks that enable key DoD capabilities and services. Adversaries may seek to cause harm to mission-critical functions by damaging the confidentiality, integrity, or availability of information and information systems, services, or networks.
- **Be alert for:** Be alert for unauthorized cyber activity including phishing and other social engineering methods.

Financial Services

- **Know:** Most of this sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Actors have the potential to disrupt critical financial systems, even inadvertently.
- **Be alert for:** Suspicious transactions or attempts to elicit financial information.

Report threats to your security officer or local Counterintelligence Office:

- Any unauthorized access to facilities, personnel, or information systems
- All suspicious activity
- Unusual requests
- Unmarked packages
- Unusual cyber activity

Health Affairs

- **Know:** This sector includes services and information that are vulnerable to targeting by adversaries via cyber or physical means. Targets include laboratories handling biological select agents and toxins, manufacturing facilities, medical supply storage facilities, and cyber infrastructure.
- **Be alert for:** Unusual activity in and around health facilities and unusual requests for information or access.

Intelligence

- **Know:** The intelligence sector includes classified or sensitive information about DoD activities, methods, and sources that directly affect mission capability, loss of which places the national defense at risk. The threat from adversary's illegally exploiting and ex-filtrating DoD intelligence information poses an unacceptable risk.
- **Be alert for:** Attempts to illegally access DoD facilities or systems, the exploitation of foreign visits, and unusual requests for information.

Logistics

- **Know:** Most of this sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Actors also have the potential to disrupt or compromise the supply chain.
- **Be alert for:** Unusual requests for information or requests for access to facilities and information systems.

Personnel

- **Know:** This sector is defined as "The DoD, government, and private Sector worldwide network that coordinates and supports personnel and human resource functions of DoD personnel." Continuity is required to ensure missions can be accomplished and to protect personnel and human capital assets from all threats.
- **Be alert for:** Attempts to illegally access DoD facilities or systems, social engineering and elicitation activities, and suspicious or unattended packages.

Public Works

- **Know:** This sector includes water, sewer, energy supply and other basic functional activities on DoD installations and facilities. The threats are manifold as public works rely upon personnel, information technology/industrial control systems, and physical infrastructure all of which are subject to illicit access, penetration, or molestation.
- **Be alert for:** Unusual activity in and around defense facilities including surveillance activity, unmarked packages, and unusual requests for information or access

Space

- **Know:** Most of this sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Actors have the potential to disrupt critical systems, even inadvertently.
- **Be alert for:** Unusual requests for information or requests for access to facilities and information systems.

Transportation

- **Know:** This sector includes aviation, highway and motor carrier, maritime, mass transit, and railway systems. Threats include terrorism, vandalism, theft, technological failures, and accidents. Cyber threats to the sector are of concern because of the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation.
- **Be alert for:** Unusual activity in and around defense transportation hubs including surveillance activity, unmarked packages, and unusual requests for information or access.

Resources

National Policy

HSPD7, Critical Infrastructure Identification, Prioritization and Protection

DoD Policy

DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)

DoD Policy

DoDD 3020.40, DoD Directive 3020.40 Mission Assurance (MA)

DoDI 5240.19, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)

DoD Web Sites

DSS CDSE Counterintelligence Training
USD(I) DCIP