REPORTING

Most of us may struggle at times. Ensure they get the help they need when appropriate. Seek positive outcomes when you can. You are the first line of defense against insider threats. Help protect our national security by reporting any suspicious behavior that may relate to an insider threat.

Each employee is responsible for ensuring the protection of classified and CUI entrusted to them.

Be aware of potential issues and actions of those around you and report suspicious behaviors and activities to your local security official/facility security officer.

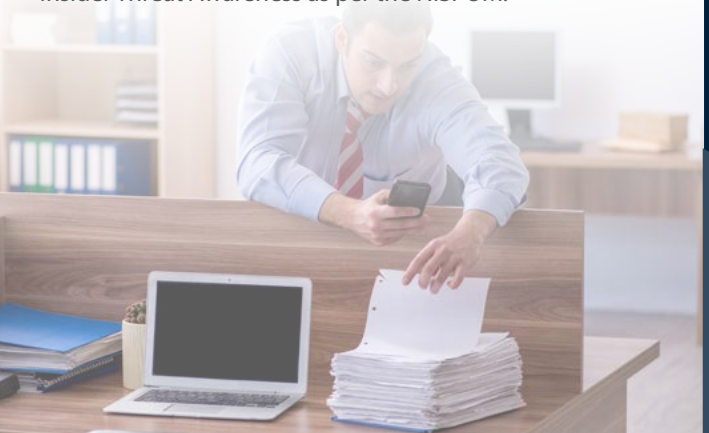
An insider can have a damaging impact on national security and industry such as:

- Loss or compromise of classified or CUI
- Weapons systems cloned, destroyed, or re-engineered
- Loss of U.S. technological superiority
- Economic loss or company bankruptcy
- Loss of company proprietary information
- Company's loss of a competitive advantage

REPORTING REQUIREMENTS

The NISPOM requires reporting suspicious contacts, behaviors, and activities. If you suspect you or your company has been targeted, report it immediately. Recognizing/reporting indicators is critical to disrupting CI threats and mitigating risks. Reporting allows us to share and address risks together.

Cleared contractors are required to receive training on Insider Threat Awareness as per the NISPOM.



DCSA
https://www.dcsa.mil

DCSA, Counterintelligence Directorate
https://www.dcsa.mil/mc/ci

Center for Development of Security Excellence
https://www.cdse.edu

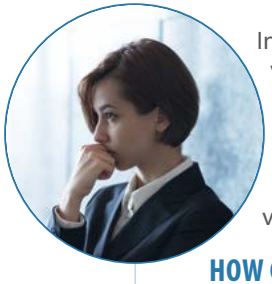
EXPLOITATION OF INSIDER ACCESS

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DEFINITIONS



Insider: Any person with authorized placement and access (P&A) to any U.S. Government or contract resource to include personnel, facilities, information, equipment, networks, or systems. This can include employees, former employees, consultants, and anyone with P&A.

- Department of Defense Directive (DODD) 5205.16: Any person with authorized access to DOD resources by virtue of employment, volunteer activities, or contractual relationship with DOD.
- Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM): Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

Insider Threat: The danger that an insider will use their P&A, wittingly or unwittingly, to harm U.S. security.

- DODD 5205.16: The threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
- NISPOM 32 CFR Part 117: The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

WHY ARE NEFARIOUS ACTIVITIES EFFECTIVE?

Insiders have arguably caused more damage to United States security than foreign intelligence officers or co-optees, and with today's technological advances, insiders with P&A and intent to damage can cause more harm than ever before. Activities that previously took years to collect targeting information now take only minutes due to increased use of removable media.

Insiders are often aware of your company's vulnerabilities and can exploit that knowledge to their benefit. Not every suspicious circumstance or behavior represents an insider threat, but every situation should be examined to determine potential risks and potentially exploitable vulnerabilities.

HOW CAN YOU RECOGNIZE AN INSIDER THREAT?

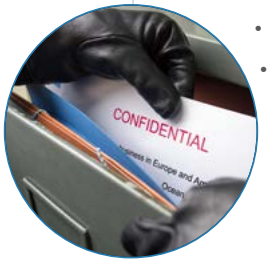
Identifying potentially malicious behavior by employees with P&A to classified or controlled unclassified information (CUI) involves gathering information from numerous sources and analyzing the data for concerning behaviors or clues. In most cases, co-workers admit they noticed suspicious or questionable activities but failed to report incidents. They made this personal decision because they did not acknowledge the insider threat patterns, or did not want to get involved or cause problems for their co-workers. Their failures to dutifully report caused grave issues for their company. Reporting insider threat is a requirement, not a choice.

A single counterintelligence (CI) indicator may say little; however, when combined with other CI indicators, it could reveal a detectable behavior pattern.

Ignoring questionable behaviors can only increase the insider's potential damage to national security or threaten employee safety. While every insider threat's motives may differ, the CI indicators are generally consistent.

POTENTIAL ESPIONAGE OR RISK INDICATORS

- Repeated security violations or a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain a higher security clearance or expand access outside job scope without need
- Engaging in classified conversations without a need to know
- Attempting to enter classified or restricted areas without authorization
- Working hours inconsistent with job assignment or unusual insistence on working in private
- Accessing information not needed for job
- Asking sensitive questions outside of "need to know" purview
- Foreign visitors wandering away from their escort at cleared contractor facilities



Behavioral Indicators:

These behaviors may also indicate potential workplace violence.

- Depression
- Excessive stress in personal life (perceived life crisis)
- Fiscal irresponsibility or financial distress
- Unexplained affluence

Exploitable Behavior Traits:

- Abusive use of alcohol or illegal/prescription drugs
- Uncontrollable gambling
- Prior disciplinary issues

REPORTABLE BEHAVIORS

Information Collection:

- Keeping classified materials in an unauthorized location (e.g., at home)
- Attempting to access classified information without authorization
- Obtaining access to sensitive information inconsistent with present duty requirements
- Questionable downloads
- Unauthorized use of removable media
- Maintaining unauthorized backups

Information Transmittal:

- Using an unclassified medium to transmit classified material
- Discussing classified materials on a non-secure telephone or in non-secure emails or texts
- Removing classification markings from documents
- Unnecessarily copying classified material

Foreign Influence:

- Expressing loyalty to another country
- Concealing reportable foreign travel or contact
- Significant ties to family members in foreign countries