WHAT TO REPORT

INFORMATION COLLECTION:

- Keeping classified materials in an unauthorized location
- Attempting to access classified information without authorization
- Unauthorized use of removable media
- Obtaining access to sensitive information inconsistent with present duty requirements
- Questionable downloads
- Maintaining unauthorized backups

INFORMATION TRANSMITTAL:

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

FOREIGN INFLUENCE:

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

REPORTING REQUIREMENTS

CFR 32 Part 117, NISPOM requires reporting suspicious contacts, behaviors, and activities.

If you suspect you or your company have been targeted, report it immediately. Recognizing and reporting indicators is critical to disrupting CI threats and mitigating risks.

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

BE ALERT! BE AWARE!

Report suspicious activities to your facility security officer

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

Defense Counterintelligence and Security Agency

WHAT ARE INSIDER THREATS?

Insider: Any person with authorized placement and access (P&A) to U.S. Government or contract resources 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 an insider will use P&A 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.*

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

- Loss or compromise of classified information or controlled unlassified information
- 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

WHY IS EXPLOITATION OF INSIDER ACCESS EFFECTIVE?

Information collection that previously took years now takes only minutes due to removable media.

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

HOW CAN YOU RECOGNIZE AN INSIDER THREAT?

Identifying potentially malicious behavior 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 did not acknowledge insider threat patterns or did not want to get involved or cause problems. Their failures to dutifully report caused grave issues for their company. Reporting insider threats is a requirement, not a choice.

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

Ignoring questionable behaviors only increases potential damage to national security and employee safety. While every insider threat's motives differ, CI indicators are consistent.

POTENTIAL RISK INDICATORS

- Repeated security violations or general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain higher security clearance or expand access outside job scope without need
- Engaging in classified conversations without 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 unnecessary information
- Asking sensitive questions outside need to know
- Allowing physical access to unauthorized individual(s) outside normal visitor procedures/business hours
- Accessing sensitive information on personally owned devices

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

COUNTERMEASURES

We all face individual hardships; however, it is important to seek positive outcomes whenever possible. Ensure you and your colleagues get help when appropriate. You are the first line of defense against insider threats. Help protect our national security by reporting any concerning behavior that may be related to an insider threat.

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

Be aware of potential issues and actions of those around you and report concerning or anomalous behavior and activities to your local security official/facility security officer, as well as the insider threat program senior official.