

Examples of 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

Information Transmittal

- Using an unclassified medium to transmit classified materials
- Discussing classified materials on a non-secure telephone or in non-secure emails or text messages
- Removing the classification markings from documents
- Unnecessary copying of classified material

Foreign Influence

- Expressing loyalty to another country
- Concealing reportable foreign travel or contact

Additional Suspicious Behaviors

- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Being disgruntled to the point of wanting to retaliate
- Repeated or unrequired work outside of normal duty hours
- Bringing an unauthorized electronic device into a controlled area
- Making threats to the safety of people or property



The above list of behaviors is a small set of examples. While not all of these behaviors are definitive indicators that the individual is an insider threat, reportable activities should be reported before it is too late.

How Can You Help?

You are the first line of defense against insider threats. Help protect our national security by reporting any suspicious behavior that may be related to an insider threat.

Each employee has a responsibility to ensure the protection of classified and controlled sensitive information entrusted to them.

Be aware of potential issues and the actions of those around you and report suspicious behaviors.

Be Alert! Be Aware!

Report suspicious activity to your local security official.



Insider Threat



Defense Security Service
Counterintelligence Directorate
www.dss.mil

COMBATING THE ENEMY WITHIN YOUR ORGANIZATION

What is an Insider Threat?

Insiders have arguably caused more damage to the security of the United States than foreign intelligence officers, and with today's technological advances, they have the ability to cause more harm than ever before.

What used to take years to collect now takes minutes because of the 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 needs to be examined to determine the potential risk.

Definitions

Insiders: Any person with authorized access to any government or contract resource to include personnel, facilities, information, equipment, networks or systems. This can include employees, former employees, consultants, and anyone with access.

Insider Threat: The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities.



Why is the Insider Threat Significant?

An insider can have a negative impact on national security and industry resulting in:

- Loss or compromise of classified or controlled sensitive information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Physical harm or loss of life

How to Recognize an Insider Threat

Detecting potentially malicious behavior among employees with access to classified or controlled sensitive information involves gathering information from many sources and analyzing that information for clues or behaviors of concern. In most cases, co-workers admit they noticed questionable activities but failed to report incidents because they did not recognize the pattern and did not want to get involved or cause problems for their co-workers.

A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be evident.

Ignoring questionable behaviors can only increase the potential damage the insider can have on national security or employee safety. While each insider threat may have different motivation, the indicators are generally consistent.

Potential Espionage Indicators

- Repeated security violations and a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required to do so
- Seeking to gain higher clearance or expand access outside the job scope without bona fide need for the access
- Engaging in classified conversations without a need to know
- Attempting to enter areas not granted access to
- Working hours inconsistent with job assignment or unusual insistence on working in private
- Accessing information not needed for job

Behavioral Indicators*

- Depression
- Stress in personal life
- Exploitable behavior traits:
 - Use of alcohol or drugs
 - Gambling
- Financial trouble
- Prior disciplinary issues

*** These behaviors may also be indicative of potential workplace violence.**