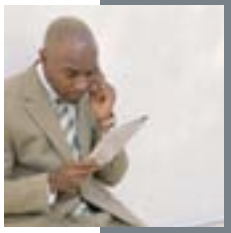
Reportable Behaviors

Information Collection:

- Keeping classified materials in an unauthorized location
- Attempting to access sensitive information without authorization
- Obtaining access to sensitive information inconsistent with present duty requirements

Information Transmittal:



- Using an unclassified medium to transmit classified materials
- Discussing classified materials on a non-secure telephone
- Removing classification markings from documents

Additional Suspicious Behaviors:

- Repeated or un-required work outside of normal duty hours
- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Attempting to conceal foreign travel

The above list of behaviors is a small set of examples. You should report any additional observed behaviors that may parallel or exceed the concerns listed in this brochure.

It is better to have reported overzealously than never to have reported at all.

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, export-controlled, or proprietary information**
- **Weapons systems cloned, destroyed, or countered**
- **Loss of technological superiority**
- **Economic loss**
- **Loss of life**

How can YOU **help?**

You and your colleagues are the first line of defense against espionage. Help protect our national security by reporting any suspicious behavior that may be related to a potential compromise of classified information.

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

Report suspicious activity to your local security contact.
Your DSS point of contact is:

INSIDER THREATS

Combating the ENEMY within your organization

This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

What is an INSIDER THREAT?

It is a sad reality, but the United States has been betrayed by people holding positions of trust.

Arguably, "insiders" have caused more damage than trained, foreign professional intelligence officers working on behalf of their respective governments.

This brochure is intended to help contractors within the National Industrial Security Program recognize possible indications of espionage being committed by persons entrusted to protect this nation's secrets.

Not every suspicious circumstance or behavior represents a spy in our midst, but every situation needs to be examined to determine whether our nation's secrets are at risk.

DSS defines insider threat as:

Acts of commission or omission by an insider who intentionally or unintentionally compromises or potentially compromises DoD's ability to accomplish its mission. These acts include, but are not limited to, espionage, unauthorized disclosure of information, and any other activity resulting in the loss or degradation of departmental resources or capabilities.

How BIG **is the problem?**

Spies have been damaging U.S. national interests since the American Revolution with Benedict Arnold. But many things about today's world make the opportunity to commit espionage from within even easier:

- Increase in the number of personnel with access to sensitive information
- Ease of transmitting information (e.g., the Internet)
- Growing demand for sensitive information from multiple "customers"

Why do people **SPY?**

- Need or desire for money
- Conflicting ideologies or disaffected political sympathies
- Psychological factors (e.g., exaggerated desire for adventure/excitement, ego gratification, misplaced anger, etc.)

How do you recognize an INSIDER THREAT?

Potential Espionage Indicators:

- Failure to report overseas travel or contact with foreign nationals
- Seeking to gain higher clearance or expand access outside the job scope
- Engaging in classified conversations without a need-to-know
- Working hours inconsistent with job assignment or insistence on working in private
- Exploitable behavior traits
- Repeated security violations
- Attempting to enter areas not granted access

Not every person who exhibits one or more of these indicators is involved with illicit behavior, but most of the persons who have been involved with espionage were later found to have displayed one or more of these indicators.

Commonalities of those who have **committed espionage since 1950:**

- More than 1/3 of those who committed espionage had no security clearance
- Twice as many "insiders" volunteered as were recruited
- 1/3 of those who committed espionage were naturalized U.S. citizens
- Most recent spies acted alone
- Nearly 85% passed information before being caught
- Out of the 11 most recent cases, 90% used computers while conducting espionage and 2/3 used the Internet to initiate contact