Insider Threat

An insider threat uses authorized access, wittingly or unwittingly, to harm national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

Insiders are able to do extraordinary damage to their organizations by exploiting their trusted status and authorized access to government information systems.

In one report on known U.S. spies, these individuals:

- Demonstrated behaviors of security concerns: 80% of the time
- Experienced a life crisis: 25% of the time
- Volunteered: 70% of the time

Although the vast majority of people are loyal and patriotic, the insider threat is real and we must be vigilant in our efforts to thwart it.

Deterring Insider Threats

We defend against the damage insider threats can cause by *deterring* insiders from becoming threats. DoD and Federal policies require agencies to establish Insider Threat Programs aimed at deterring, detecting, and mitigating the risks associated with insider threats. Their activities include:

- Proactively identifying insiders who exhibit potential risk indicators through:
    - User activity monitoring
    - Workplace reporting
- Formulating holistic mitigation responses to decrease risk while achieving positive outcomes for the organization and the individual. For example:
    - Referring individuals to counseling or other types of assistance to alleviate personal stressors
    - Requiring training on security protocols
    - Developing organization-wide protocols designed to secure information, resources, and personnel

Detecting Insider Threats

We detect insider threats by using our powers of observation to recognize potential insider threat indicators. These include, but are not limited to:

- Difficult life circumstances
  - Divorce or death of spouse
  - Alcohol or other substance misuse or dependence
  - Untreated mental health issues
  - Financial difficulties
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Unexplained or sudden affluence
- Unreported foreign contact and travel
- Inappropriate, unusual, or excessive interest in sensitive or classified information
- Mishandling of classified information
- Divided loyalty or allegiance to the U.S.

Reporting Requirements

Individuals experiencing stressful situations may be vulnerable to exploitation. To protect against the insider threat, be alert to and report any suspicious activity or behavior or potential security incident in accordance with your agency's insider threat policy to include:

- Attempt to access sensitive information without the need-to-know
- Unauthorized removal of sensitive information
- Unusual request for sensitive information
- Bringing an electronic device into prohibited areas
- Sudden purchases of high value items/living beyond one's means
- Overseas trips for no apparent reason or of short duration
- Alcohol or drug problems
- Abrupt changes in personality or workplace behavior
- Consistent statements indicative of hostility or anger toward the United States and its policies