Insider Threat

Definition

An insider threat is any person with authorized access to any US Government resources, including personnel, facilities, information, equipment, networks, or systems, who uses that access, either wittingly or unwittingly, to do harm to the security of the United States.

Other Insider Threat Concerns

- Criminal Activity including theft and fraud
- Safety including an active shooter incident
- Financial harm to industry by stealing unclassified but sensitive or proprietary information

Insider Threats May Be

- Recruited: a foreign entity may use exploitable weaknesses to convince an individual with access to provide information to those who do not have a need-to-know
- Volunteer: An individual may choose to sell out their country or organization motivated by greed, disgruntlement, divided loyalties, or ideological differences
- Unwitting: An individual may unwittingly give away information through poor security procedures or clever elicitation collection techniques

Indicators

Indicators of a potential insider threat can be broken into four categories:

1. Recruitment
2. Information Collection
3. Information Transmittal
4. Other Suspicious Behavior

❖ Report indicators to the Facility Security Officer (FSO)

1. Recruitment Indicators

- Unreported request for critical assets* outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with someone who is known or suspected of being associated with foreign intelligence, security or terrorism
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger

*Critical assets are assets essential to an organization's mission or to national security, that if exploited, could result in serious harm. They include classified information, proprietary information, intellectual property, trade secrets or personnel security.

2. Information Collection Indicators

- Unauthorized downloads or copying of files
- Keeping critical assets at home or any unauthorized space
- Acquiring unauthorized access to automated information systems
- Operating unauthorized cameras, recording devices, computers or modems in areas where critical assets are stored, discussed or processed
- Requesting access to critical assets when not authorized
- Asking for witness signatures certifying the destruction of classified information without observing the destruction

3. Information Transmittal Indicators

- Removing critical assets from the work area without authorization
- Extensive use of copy, fax, or computer equipment to reproduce or transmit critical asset-related information exceeding job requirements
- Using an unauthorized means to transmit classified information (including discussions in unauthorized spaces)
- Attempting to conceal any work-related or personal foreign travel
- Improperly removing classification markings from documents

4. Other Suspicious Behaviors

- Attempts to expand access to critical assets through volunteering for assignments beyond the normal scope of responsibilities
- Questionable behavior that results in repeated security violations, or engaging in illegal activity or coercing others to engage in illegal activity
- Unexplained changes in financial circumstances
- Attempts to compromise others who have access to critical assets or to place them under personal obligation through favors, gifts, money, or other means

Other Suspicious Behaviors (cont.)

- Questionable loyalty to the US government through anti-American comments
- Questionable loyalty to RED-INC through exhibited behaviors associated with disgruntled employees (e.g., conflicts with supervisors and coworkers, decline in work performance, tardiness, or unexplained absenteeism)

Reporting Requirements

- Suspected insider threats must be reported to the company FSO
- When you fail to report, you risk the physical security of yourself and the information security of our company and the contracts we work. Insider threats weaken the US military's battlefield advantage and jeopardize the war fighter. They increase our vulnerability to fraud, terrorist activity and cyber-attacks. As an employee of a federal contractor failure to report could cost our company contracts…and that indirectly threatens your job.

Reporting Requirements (cont.)

- Failing to report also fails the employee who needs help. When you don't report, you lose the opportunity to help your coworker resolve problems before committing espionage or hurting others.
- Failure to report could cost you your clearance and your job and may result in criminal charges.
- Don't underestimate the seriousness of the insider threat to our national security or the role you play in protecting against insider threats.