The Insider Threat and Its Indicators

What is an Insider Threat?

An insider threat is any person with authorized access to any U.S. 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 U.S.

Other insider threat concerns may include:

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

For the purposes of the NISPOM, insider threat refers to the threat of an insider using his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of government, company, contract or program information, resources or capabilities.

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 because of motivators such as greed, disgruntlement, divided loyalties, or ideological reasons.
- 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--indicators of: recruitment, information collection, information transmittal and general suspicious behavior. Keep in mind that not all insider threats exhibit all of these behaviors and not all instances of these behaviors indicate an insider threat.

Recruitment

Reportable indicators of recruitment include, but are not limited to:

- Unreported request for critical assets[1] outside official channels
- Unreported or frequent foreign travel
- Suspicious foreign contacts
- Contact with an individual who is known to be, or is suspected of being, associated with foreign intelligence, security, or terrorism
- Unreported offer of financial assistance, gifts, or favors by a foreign national or stranger: *Beware of those bearing gifts*

Information Collection

Reportable indicators of information collection include, but are not limited to:

- Unauthorized downloads or copying of files, especially for employee who have given notice of termination of employment
- Keeping critical assets at home or any other unauthorized place
- Acquiring access to automated information systems without authorization
- Operating unauthorized cameras, recording devices, computers, or modems in areas where critical assets are stored, discussed, or processed
- Asking you or anyone else to obtain critical assets to which the person does not have authorized access
- Seeking to obtain access to critical assets inconsistent with present duty requirements
- Asking for witness signatures certifying the destruction of classified information when the witness did not observe the destruction

[1] "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; personnel security.

Information Transmittal

Reportable indicators of information transmittal include, but are not limited to:

- Removing critical assets from the work area without appropriate authorization
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit critical asset-related information that may exceed job requirements
- Discussing critical asset-related information in public or on a nonsecure telephone

Information transmittal actions/behaviors specific to classified information:

- Using an unauthorized fax or computer to transmit classified information
- Attempting to conceal any work-related foreign travel and any personal foreign travel while having a Top Secret/Sensitive Compartmented Information clearance or being a contractor with a reporting requirement
- Improperly removing the classification markings from documents

Other Suspicious Behaviors

Reportable indicators of other suspicious behaviors include, but are not limited to:

- Attempts to expand access:
    - Attempting to expand access to critical assets by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
    - Performing repeated or unrequired work outside of normal duty hours, especially unaccompanied
- Questionable behavior:
    - Exhibiting behavior that results in repeated security violations
    - Engaging in illegal activity or asking you to engage in any illegal activity
- Changes in financial circumstances:
    - Displaying unexplained or undue affluence explained by inheritance, luck in gambling, or some successful business venture
    - Displaying sudden reversal of financial situation or sudden repayment of large debts
- Attempts to compromise individuals:
    - Attempting to entice personnel with access to critical assets into situations that could place them in a compromising position
    - Attempting to place personnel with access to critical assets under obligation through special treatment, favors, gifts, money, or other means

- Questionable national loyalty:
    - Displaying questionable loyalty to U.S. government or company
    - Making anti-U.S. comments
- Exhibits actions or behaviors associated with disgruntled employees:
    - Conflicts with supervisors and coworkers
    - Decline in work performance
    - Tardiness
    - Unexplained absenteeism