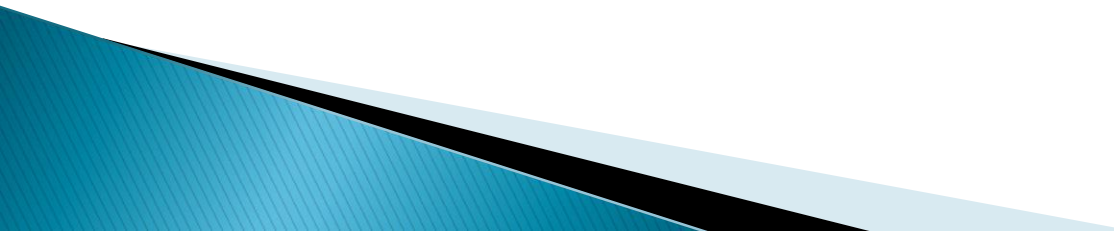


# Insider Threat Awareness Training

# 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 any one with access.
  - ▶ **Insider Threats:** The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation or government, company, contract program information, resources, or capabilities.
- 

# General Suspicious Behavior

## **Attempt to Expand Access:**

- ▶ Attempting to expand access to critical assets by repeatedly volunteering for assignments of duties beyond the normal scope to 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
- ▶ Bringing an unauthorized electronic device into a controlled area

## **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 situations 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

# Psychosocial Indicators

## Disgruntlement

- ▶ Responds poorly to criticism
- ▶ Inappropriate response to and/or inability to cope with stress at work
- ▶ Sudden change in work performance

## Emotional

- Change in beliefs
- Unusual level of pessimism
- Unusual level of sadness
- Difficulty controlling emotions


## Ego

- Domineering
- Harassment
- Argumentative
- Superiority Complex
- Selfish
- Manipulative
- Rules don't apply
- Poor teamwork
- Irritability
- Threatening
- Retaliatory behavior

## Relationship/Financial Problems

- Divorce
- Marriage problems
- Stress at home
- Financial Problems
- Inappropriate response to and/or inability to cope with stress at home
- Unexplained change in financial status
- Irresponsibility

# Reportable Indicators of Recruitment Include, But Not Limited to:

- ▶ Unreported request for critical assets 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 nation or stranger: *Beware of those bearing gifts*
  - ▶ Suspected recruitment by foreign or domestic competitive companies to convince employee to work for another company
- 

# Reportable Indicator of Information Collection Include, But Are Not Limited to:

- ▶ Unauthorized downloads or copying of files, especially for employees 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

## **Actions/behaviors specific to classified information:**

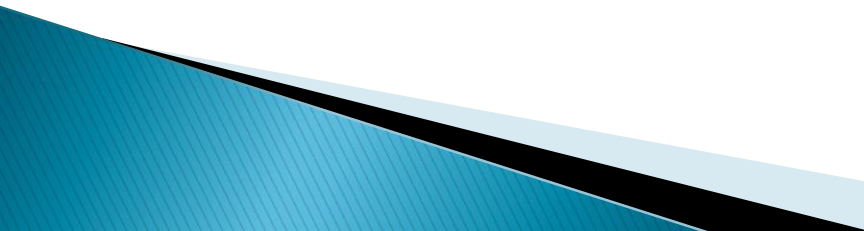
- ▶ Asking for witness signatures certifying the destruction of classified information when the witness did not observe the destructions

# Information Transmittal Indicators

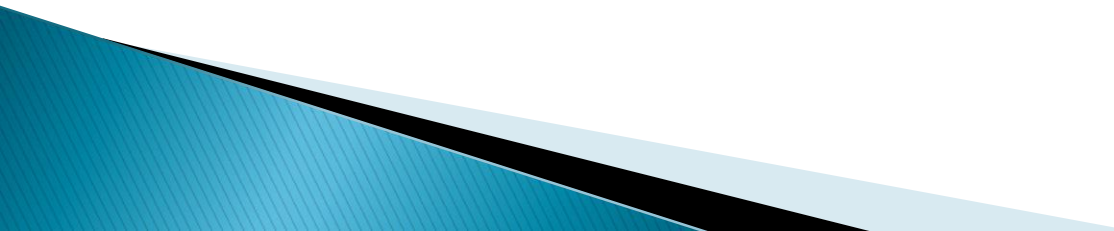
## **Reportable Indicators of Information Transmittal Including, but Not Limited to:**

- ▶ Removing critical asset from the work area without appropriate authorization
- ▶ Extensive use of copier, fax, 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 phone

## **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 of being a contractor with a reporting requirement
  - ▶ Improperly removing the classification markings from documents
- 

# Lessons Learned

- ▶ Insider threats are not from hackers
  - ▶ Insider threat is not a technical or “cyber security” issue alone
  - ▶ A good insider threat program should focus on deterrence, not detection
  - ▶ Detection of insider threats has to use behavioral based techniques
- 



if you  
**SEE** | **SAY**  
something | something

REPORT SUSPICIOUS BEHAVIOR  
TO LOCAL SECURITY CONTACT