Insider Threat Program
Awareness Briefing

Security Manager
Thomas Metzger, SFPC, SAPPC, PSC

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Insider Threat Program
Goals

At the end of this brief, you will be able to:

• Understand the importance of detecting potential insider threats and reporting behaviors of concern to insider threat personnel or other designated officials

• Describe methodologies of adversaries to recruit trusted insiders and collect information (classified and unclassified)

• Identify indicators of insider threat behavior and procedures to report such behavior

• Understand counterintelligence and security reporting requirements

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
The threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
Insider Threat Program

History of Recent Incidents

• Fort Hood Shooting (2009) U.S. Army Major Nidal Hasan
  • Fatally wounded 13
  • 30 more injured
  • Why? Unhappy with the U.S. involvement in Afghanistan and Iraq

• Petty Officer Bryan Martin (2010) Attempted Espionage
  • Attempted to sell classified documents
  • Pled guilty to four counts of attempted espionage
  • Why? “Blinded by greed” - Ultimately paid only $11,500.00 (by undercover agents)

• Pearl Harbor Shooting (2019) Seaman Gabriel Romero
  • USS COLUMBIA (SSN 771) Topside Sentry
  • 2 killed, 1 wounded
  • Why? No answer

• USS MIAMI (SSN 755) Fire/Arson (2012) Casey J. Fury
  • Fire started intentionally
  • $450 Million in damage and Loss of U.S. Strategic Asset.
  • Sentenced to 17 years confinement / $400 Million in restitution

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Insider Threat Program
DoD and DoN Insider Threat Program

• **National Insider Threat Program**
  – Executive Order 13587 (EO 13587)
    • Establishes National Program

• **Department of Defense (DOD) Insider Threat Program**
  – DODD 5205.16
    • “Leverages counterintelligence (CI), security, cybersecurity, Human Resources (HR), Law Enforcement (LE), and other relevant functions and resources to identify and counter the insider threat”

• **Department of the Navy (DoN) Insider Threat Program**
  – SECNAVINST 5510.37
    • Establishes the DoN Insider Threat Program
**Insider Threat Program**

*What is an Insider Threat*

- **Navy definition:**
  - "a person with authorized access who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities."

- **Simply put, an insider threat means:**
  - Unauthorized or unlawful disclosure of classified information that damages the national security
  - Violence that results in injury, loss of life and/or damage to Navy Resources
Internal Threat

The trusted employee we come in contact with every day –
Not necessarily members of the cleared community!
No environment is immune from insider threat.

Threats may include:

- Espionage
- Unauthorized Disclosure
- National Security Crimes
- Workplace Violence
- Sabotage
- Fraud
- Security Violations
- Unwitting Actions that increase vulnerabilities
- Other Counterproductive workplace activity

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
**Inside Threat Program**

**Potential Risk Indicators**

Most employees engaging in threat behavior showed one or more Potential Risk Indicators (PRIs).

Potential Risk Indicators may include but are not limited to:

<table>
<thead>
<tr>
<th>Ignorance</th>
<th>Complacency</th>
<th>Malice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lack of awareness of policies and procedures creates risk</strong></td>
<td><strong>Lax approach to policies and procedures creates risk</strong></td>
<td><strong>Malicious and intentional acts create risk</strong></td>
</tr>
</tbody>
</table>

**Examples include:**

- Unknowingly clicking on a phishing scam
- Attaching passwords to his/her laptop
- Leaving sensitive information on his/her desk unattended
- Discussing sensitive information in a public location
- Failing to adhere to obligations in understanding what is sensitive information and protecting it
- Unknowingly committing security infractions or violations
- Misusing Government IT systems for non-work functions
- Using personal storage devices (e.g., phones, laptops, iPads) for conducting official business without authorization
- Uploading sensitive files to a third party site
- Allowing unknown individual inside the door behind him/her without a badge
- Unauthorized absences
- Unreported foreign contacts or travel
- Drug or unauthorized alcohol use in the workplace
- Possessing unauthorized weapon in the workplace

**Overall Classification:** UNCLASSIFIED//FOR OFFICIAL USE ONLY
Observable and Reportable Potential Risk Indicators (PRIs) may fall into the following categories:
Potential risk indicators related to security violations include:

- Establishing pattern of security violations
- Seeking to expand access
- Being reluctant to submit to polygraph
- Being responsible for unaccounted for classified materials
- “Fishing” through offices, desk drawers, files, and storage containers in search of classified material
Intentional Mishandling of Classified Information

- Attempts to Obscure Classification Markings
- Unauthorized Removal of Classification Markings
- Classified Materials Kept at Home or Taken on Trips
- Retention of Classified, Export Controlled or Other Sensitive Materials obtained at Previous Jobs

Ben-ami Kadish, December 2008: Pled guilty to acting as unregistered agent of foreign power.

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Misuse of IT Systems

- Accessing or Attempting to Access Systems Outside of Normal Work Hours
- Repeated Deviations from or Circumventions of Standard Security Procedures
- Use of Unmarked Electronic Media Containing Classified Information
- Unexplained or Out of the Ordinary Changes in System or User Activity
- Use of Numerous Passwords and Log Ins
- Attempting to Obtain the Passwords of Coworkers
- Browsing Files and/or Records Not Authorized

Michael Mitchell, December 2009: Pled guilty to trade secret theft.

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Potential risk indicators related to suspicious behavior include:

- Working hours inconsistent with job assignment
- Insisting on working in private without a valid reason
- Demonstrating exploitable behavior traits
- Revealing unexplained affluence
- Showing infatuation with covert activity and interest in clandestine operations
Foreign Preference/Loyalty

- Strong Ties or Affiliations to Foreign Nations
- Ownership of Property or other Vested Economic Interest Abroad
- Attempts to Conceal Service in Foreign Military, Gov’t, or Intel Service

Chi Mak, May 2007: Convicted of conspiracy and other violations. Sentenced to 24 years.
Foreign Contacts

- Contact with Foreign Officials and Representatives
- Visits to Official Foreign Establishments for Unexplained Reasons
- Attempts to Conceal Contacts with Foreigners
- Visits to Foreign Diplomatic Facilities

Elliot Doxer, December 2011: Sentenced to 6 months prison, 6 months home confinement & $25,000 fine for economic espionage.

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Insider Threat Program
PRI: Suspicious Behavior

Unexplained Affluence

- Sudden Purchase of High Value Items
- Unexplained Ready Cash
- Unexplained Settlement of Large Outstanding Debts
- Large Deposits to Savings Accounts
- Opening of Savings or Stock Accounts with Foreign Banks

Wen Chyu Liu, January 2012:
Sentenced to 60 months prison, $25k fine and forfeiture of $600k.
Trade secret theft to China.

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Potential risk indicators related to unexplained foreign travel include:

- Reported/unreported foreign travel and contact with foreign nationals
- Routine vacations to countries of interest
- Frequent, unexplained short trips
Frequent Unexplained Trips
of Short Duration

- Frequent, Unexplained, Short
- Not Necessarily Foreign Destinations!

Jin Hanjuan
August 2012: Sentenced to four years for corporate espionage.
Foreign anomalies include:

- Appearance of classified or proprietary technology
- Equipment or technology that incorporate protected U.S. technology
- Foreknowledge of U.S. diplomatic positions, negotiating strategies, or troop movements
- Knowledge of sensitive U.S. projects, programs, or technologies by name or designator
- Publication of classified or sensitive U.S. information
- Implementation of countermeasures
Threats of Physical Violence or Harm

- Disgruntlement
- Substandard performance
- Frequent fights with coworkers and supervisors
- Failure to follow regulations and guidelines
- Displays of ill temper and false accusations against others
- Repeated reprimands, disciplinary sanctions

Ivan Lopez
April 2, 2014:
Killed 3 soldiers and wounded 14 others.

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Other Indicators

- Contact with Foreign Intelligence Service
- Deception Indicated on CI Polygraph
- Membership in Subversive Group/Organization
- Unauthorized Absences
- Criminal Affiliations
- Disgruntlement
- Paranoid behavior
- Working hours inconsistent with job assignment
- Insists on working alone/private
- Loyalty questioned
- Rummaging through offices/desks

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
CDSE CI Awareness Video

https://www.youtube.com/watch?v=IBH4ddYxKyg
Insider Threat Program
Foreign Targeting and Recruitment

- **Spot and Assess**
  
  Foreign Intelligence Entities (FIE) spot and assess individuals for potential recruitment. Adversaries are not necessarily looking for someone with a high level of access; sometimes the potential for future access or the ability of the recruit to lead to other high value targets is enough to generate adversary interest. Spotting and Assessing can take place anywhere, but is always approached in a non-threatening and natural manner: Trade shows, business contacts, social events, or online venues such as chat rooms and social media, are used for this process. During this phase, the FIE will often explore potential exploitable weaknesses which may be used as leverage against the recruit. These could include: **Drugs or Alcohol, Gambling, Adultery, Financial Problems**, or other weaknesses.

- **Develop**
  
  Once a potential recruit has been identified, adversaries begin to cultivate a relationship with that individual in the “Development Phase”, meetings with the recruit become more private and less likely to be observable or reportable. By the time the “recruitment and handling” phase is initiated, the individual is likely emotionally tied to the adversary.

- **Recruit**
  
  The actual recruitment may involve appeals to ideological leanings, financial gain, blackmail or coercion, or any other of a number of motivators unique to that recruit. Some of these may manifest as observable and reportable behaviors.

- **And/Or Elicit**
  
  Not all FIE Targeting ends in recruitment. Sophisticated social engineering efforts include personal elicitation of information and targeted online phishing campaigns can be used to gather information from source.
Insider Threat Program
Potential Terrorist Indicators

- Spending abnormal amounts of time with others in the group
- Long absences from their immediate locality
- Trouble with employment
- Trouble keeping employment
- Criminal activity
- Unexplained Affluence
- Changes in character, behavior, appearance
- Strong ideological beliefs

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Opportunity and crisis contribute to vulnerability.

Access

Potential Risk Indicators

Perceived Life Crisis

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Insider Threat Program
Opportunity, Motive, Ability, Trigger

PRIs
- Accessing information outside need to know
- Repeatedly borrowing money from coworkers
- Mishandling Classified Information
- Anti-social behavior, narcissism, risk taking

Perceived Life Crisis
- Massive Gambling Debt

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Not everyone that exhibits indicators is an Insider Threat!
DoD Reporting Requirements:

- Identify and report indicators of illicit foreign collection activity
- Identify and report illicit foreign cyber activities
- Identify and report potential espionage indicators
- Identify and report factors contributing to insider threat vulnerability
DoD personnel who fail to report information that identifies reportable contacts, activities, indicators and behaviors, may be subject to judicial or administrative action (or both), pursuant to applicable law and regulations.

- Military: UCMJ: Punitive action under Article 92
- Civilian Employees: Appropriate disciplinary action under regulations governing civilian employees.
Insider Threat Program
NAVFACSW Specific Reporting:

• Governing instruction: SECNAVINST 5510.37

• NAVFACSW Insider Threat / Security/ Counterintelligence Reporting Contact:
  Mr. Thomas Metzger, Security Manager
  (619)532-2913
  thomas.metzger@navy.mil

• NCIS Tip Line:
  • Text “NCIS” + tip info to CRIMES (274637)
  • “Tip Submit” Andriod and iPhone App (Select NCIS as agency)
  • Call 1-800-543-Navy (6289)

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
Insider Threat Program
Summary

• Understand the importance of detecting potential insider threats and reporting of suspected activity to insider threat personnel or other designated officials

• Describe methodologies of adversaries to recruit trusted insiders and collect classified information

• Identify indicators of insider threat behavior and procedures to report such behavior

• Understand counterintelligence and security reporting requirements

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY
QUESTIONS?