Potential Risk Indicators: Insider Threat

What is the "something" we should be looking for?

Insider Threat – Potential Risk Indicators (PRI)

What is an Insider Threat?

An Insider Threat is anyone with authorized access who uses that access to wittingly or unwittingly harm the organization and its resources. Insiders can be employees, vendors, partners, suppliers, etc.; they are individuals that you provide access to your facilities and/or information. Trusted insiders may commit malicious acts, such as fraud, theft, sabotage, espionage, unauthorized disclosure, workplace violence, and more. Unwitting insiders may inadvertently disclose sensitive information, unknowingly download malware, or facilitate other cybersecurity events. Anyone can be a potential insider threat. All organizations are vulnerable.

Potential Risk Indicators

Most insider threats exhibit risky behavior prior to committing negative workplace events. If identified early, many risks can be mitigated before harm to the organization occurs. It is your responsibility to report these indicators to your supervisor, security officer, and/or insider threat program.

Spotting and Reporting PRI

Not all of these potential risk indicators will be evident in every insider threat and not everyone who exhibits these behaviors is doing something wrong. However, most of insider threats have displayed at least some of the potential risk indicators.

Early reporting allows the Insider Threat Program to pursue a multi-disciplinary approach to gathering and reviewing information indicative of an insider threat, referring that data as appropriate, and developing mitigation response options while protecting the privacy and civil liberties of the workforce. The goal of the program is to deter threats and detect potential issues early on—before a problem occurs. Early reporting can prevent harm to self or others, losses to the organization, and protect national security.

Consult the following resources for additional information on insider threat indicators and reporting:

INT 101 course

Insider Threat Vigilance Resources

Insider Threat Potential Risk Indicators

Access Attributes

- **Security clearance and information access**
  - o **Confidential**
  - o **Secret**
  - o **TS**
  - o **SCI, SAP, etc.**
- **Access to physical facilities**
  - o **Secret-cleared spaces**
  - o **SCIF, SAP, etc.**
- **Access to systems and applications**
  - o **SIPR and other Secret**
  - o **JWICS or other SCI, SAP, etc.**
- **DoD system(s) privileged user**
- **Explosives access or training**
  - o **Training**
  - o **Physical access to material**
- **CBRN access or training**
  - o **Training**
  - o **Physical access to material**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Professional Lifecycle and Performance

- ❖ Access Attributes
- ❖ Professional Lifecycle and Performance
- ❖ Foreign Considerations
- ❖ Security and Compliance Incidents
- ❖ Technical Activity
- ❖ Criminal, Violent, or Abusive Conduct
- ❖ Financial Considerations
- ❖ Substance Abuse and Addictive Behaviors
- ❖ Judgement, Character, and Psychological Conditions

- **Declining performance ratings**
- **Poor performance ratings**
- **Reprimand/Non-Judicial Punishment**
- **Human Resources (HR) complaints**
- **Demotion**
- **Separation status**
  - **Pending voluntary separation**
  - **Pending involuntary separation**
- **Suspension**
- **Involuntary administrative leave**
- **Leave of absence**
- **Unauthorized absence/AWOL**
- **Negative characterization of previous employment or service**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Foreign Considerations

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

- **Citizenship (Threat or non-threat country – past/present)**
- **Foreign travel to countries of concern (Official or Non-Official)**
- **Frequent foreign travel (excluding official travel)**
- **Other foreign travel**
- **Service in foreign military or government**
- **Possessing foreign passport**
- **Voting in foreign election**
- **Possession of foreign assets**
- **Foreign residency**
- **Foreign business or political interest**
- **Receiving benefits from a foreign nation**
- **Foreign citizenship - spouse or cohabitant**
- **Foreign citizenship - immediate family member**
- **Living with foreign national**
- **Foreign national contact**
- **Unauthorized contact with an officer or agent of a foreign intelligence entity (FIE)**
- **Enabling or facilitating an officer, agent, or member of a FIE**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Security and Compliance Incidents

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

BACK

- **Compliance violation**
- **Security infraction**
- **Security violation**
- **Non-compliance with training requirements**
- **Delinquent Government Travel Charge Card (GTCC)**
- **Misuse of DoD purchase card or expense violations**
- **Time entry violations**
- **Security clearance denial, suspension, or revocation**
- **Misusing privileged functions**
- **Physical access anomalies**
- **Virtual access anomalies**
- **Accessing DoD physical facilities at off-hours**
- **Accessing DoD systems and applications at off-hours**
- **Attempts to obtain national security information without proper clearance**
- **Attempts to obtain national security information without need-to-know**
- **Outside employment not in accordance with official guidelines**
- **Failure to self-report required information associated with holding a security clearance**

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Technical Activity

- **Violating acceptable user or other automated information system policies**
- **Suspicious or unauthorized email or browsing activity**
- **Attempting to introduce unapproved USB device**
- **Anomalous volume of data transferred to removable media inserted in USB port**
- **Attempting to burn discs without authorization**
- **Transfer data to personal or suspicious account**
- **Erasing, modifying, or tampering with any record-keeping data**
- **Introduction of unauthorized software**
- **Attempted modification to registry or system settings**
- **Disabling anti-virus or firewall settings**
- **Introducing malicious code**
- **Technical violations admitted during investigation or polygraph**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Criminal, Violent, or Abusive Conduct

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

- **Criminal violent behavior, to include sexual assault and domestic violence or other criminal behavior**
  - **Voluntary admission, included during polygraph examination or investigation**
  - **Substantiated report or arrest**
  - **Criminal proceedings (charge or conviction)**
- **Exhibiting violence at work (directed against property or persons)**
- **Threatening violence**
- **Possessing unauthorized weapon**
- **Authorized weapon at an unauthorized time or location**
- **Weapon mishandling**
- **Criminal behavior involving weapons**
- **Failure to follow court order**
- **Parole or probation or violation thereof**
- **Criminal affiliations**
- **Self-harm, suicidal ideation, or attempting suicide**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Financial Considerations

- Financial crime
  - Voluntary admission, including during polygraph or investigation
  - Substantiated report or arrest
  - Criminal proceeding (charge or conviction)
- Filing for bankruptcy
  - Adverse changes to financial status
  - Foreclosure or repossession
  - Loan default
  - Involuntary lien or unfavorable judgement
- Delinquent debts
- High debt-to-income ratio
- Failure to file tax returns
- Pay garnishment
- Displaying signs of unexplained affluence
- Experienced gambling problem

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Substance Abuse and Addictive Behaviors

- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

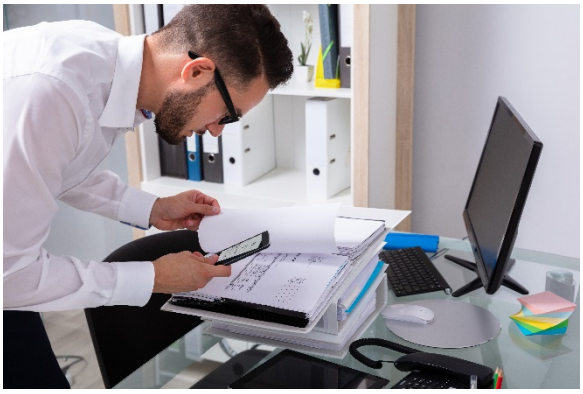
- **Illegal substance use or trafficking**
  - **Voluntary admission, including during polygraph or investigation**
  - **Drug test failure**
  - **Substantiated report or arrest**
  - **Criminal proceeding (charge or conviction)**
  - **Incident at work involving an illegal substance**
- **Legal substance abuse or trafficking (alcohol or prescription drugs)**
  - **Voluntary admission, including during a polygraph or investigation**
  - **Substantiated report or arrest**
  - **Criminal proceeding (charge or conviction)**
  - **Incident at work involving alcohol abuse or legal substance abuse**
- **Voluntary or involuntary treatment for abuse of drugs, alcohol, or controlled substances**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."

Insider Threat Potential Risk Indicators

Judgement, Character, and Psychological Conditions



- Access Attributes
- Professional Lifecycle and Performance
- Foreign Considerations
- Security and Compliance Incidents
- Technical Activity
- Criminal, Violent, or Abusive Conduct
- Financial Considerations
- Substance Abuse and Addictive Behaviors
- Judgement, Character, and Psychological Conditions

- **Falsifying hiring information**
- **Falsifying data at place of work**
- **Subject to judgement in civil litigation**
- **Expressing ill-will towards USG or employing organization**
- **Communicating extremist views**
- **Associating with extremist or terrorist groups**
- **Enabling or facilitating an extremist or terrorist group**
- **Admission to inpatient mental health facility**
  - **Voluntary**
  - **Involuntary**
- **Insanity plea in a criminal case**
- **Anti-social or compulsive behavior**
- **Mental instability**
- **Past untruthfulness (including voluntary admission, including during polygraph or investigation)**
- **Failure to successfully complete a polygraph**
- **Communicating endorsement of workplace violence**
- **Other psychiatric or psychological condition**

BACK

"You cannot underestimate the role you play in protecting against insider threats. You are the first line of defense."