Insider Threat Program Implementation

NCMS Insider Threat Subcommittee
July 2021

Disclaimer

We do not represent or speak on or behalf of the U.S. Government or Defense Counterintelligence and Security Agency.

We do not represent or speak on or behalf of our respective employer.

We do not endorse any particular product, service, or vendor.

Best Practices & Sharing of Ideas

Agenda

- The Shift from Compliance to Risk
- NISPOM v3 and Insider Threat ISL
- Insider Threat Defined, Drivers and Indicators
- Basic Requirements and Best Practices
- Self Inspections, Internal Assessments
- Potential Program Metrics
- Preparing for Meaningful Engagements
- Resources

The Shift from Compliance to Risk

What does this shift to risk mitigation mean for Industry?

Compliance* defined as conformity in fulfilling official requirements

Risk* defined as to expose to hazard or danger

- What are you doing and how? - Compliance
- Is what you're doing effective to ensure security? **Prove it….** - Risk

The shift to risk mitigation demonstrates many things - but most importantly… when developing an insider threat program, **it requires Industry to assess itself to determine what is most important within their organization and develop controls and mitigations in order to protect it and mitigate risk against it.**

The Government is responsible for developing baseline protection requirements of classified information.

Industry is responsible for implementing those classified information requirements and more!

*MerriamWebster.com

NISPOM v3 & Insider Threat ISL

NISPOM v3 (aka 32 CFR part 117)

- There are no significant changes to insider threat program requirements
- Any specific updates will most likely occur with new InT ISL
- For overview of NISPOM v3 changes, look here

Insider Threat ISL

- Based on the last draft, aligned with NITTF Maturity Framework
- Prioritization of the InT ISL has been moved to make way for NISPOM v3
- More to come from DCSA! Stay tuned!

Insider Threat Defined

NISPOM

Insider threat is defined as “the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency’s obligations to protect classified national security information.” (NISPOM Appendix C)

Best Practice

Depending on your program scope, insider threat can be defined many different ways.

Your program may not even use the term “insider threat”

- Cleared vs Uncleared Personnel
- US Govt classified information vs Company IP, other sensitive data
- Networks (Classified, Non-Classified)
- Certain facilities or All facilities

Insider Threat Defined - Examples

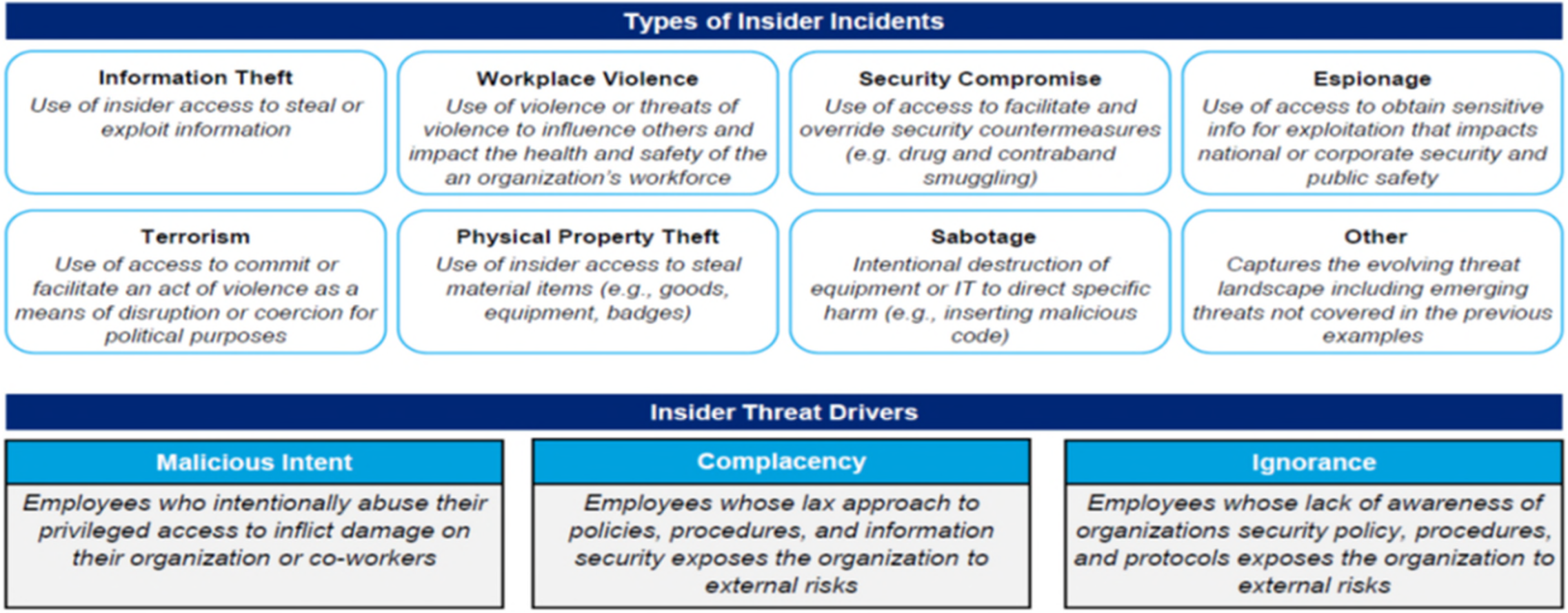
Example 1

An insider risk is anyone with access to facilities, networks or people who either intentionally or unintentionally creates damages or losses that hurt the company or people, impacting the Company's security posture or that of its customers.

Example 2

An insider threat is a security risk that originates from within the targeted organization. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organization, and who misuses the access.

Types of Incidents and Drivers



*From Deloitte 2012 Insider Threat Types

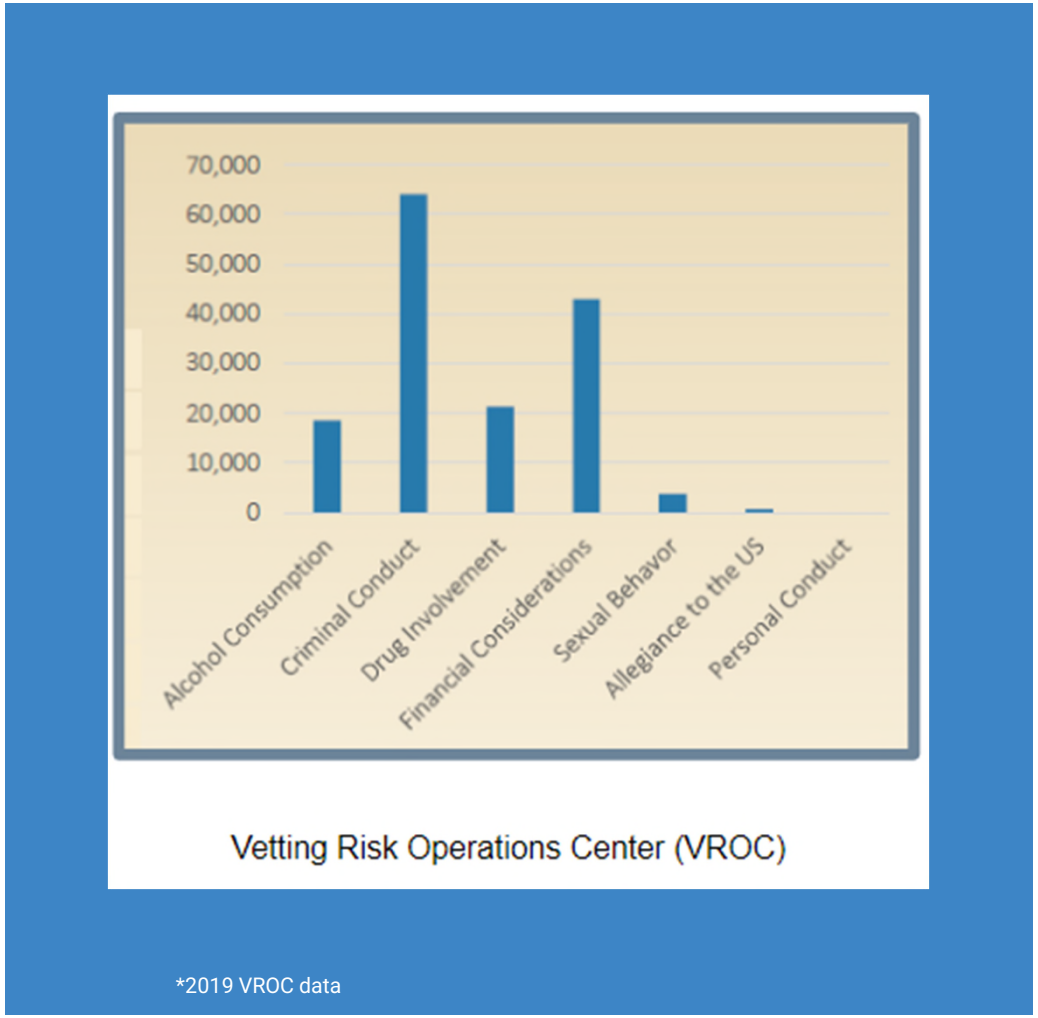
Indicators

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Considerations
- Criminal Conduct
- Handling protected Information
- Outside Activities
- Use of Information Technology

Best practice go beyond 13 Adjudicative Guidelines

- ❑ Identify the Critical Path
- ❑ Performance Improvement Plans
- ❑ Stressors

Think <u>Whole Person</u> concept!



The Basics - ITPSO

Designate an Insider Threat Program Senior Official (1-202b)

NISPOM and ISL Requirement

US Citizen employee, Cleared at the FCL level, Key Management Personnel, appointed in e-FCL (now NISS) (1-202b, ISL 2016-02 1-202b)

Must complete insider threat training (3-103a)

Responsible for establishing and executing contractor's insider threat program (ISL 2016-02, 1-202b)

Provide management, accountability and oversight to effectively implement and manage the requirements of the NISPOM related to insider threat (ISL 2016-02, 1-202b)

If using a corporate ITPSO, each cleared legal entity must appoint an ITPSO in NISS (1-202c)

Best Practice

Appointment of the ITPSO is a business decision made by Leadership and other business leaders

Depending on the size of your company and/or program:

You could need more than one ITPSO (if 1+ CAGE Code)
- East Coast vs. West Coast
- Special programs vs. collateral

The FSO could be the ITPSO

The Basics - Written Plan

Create a Written Plan (ISL 2016-2)

NISPOM and ISL Requirement

Contractors must establish and maintain an insider threat program to detect, deter and mitigate insider threats **(1-202a)**

Plan that outlines the capability to "gather, integrate and report relevant insider threat information across the contractor facility commensurate with the organization's size and operations" **(ISL 2016-02 1-202a)**

Develop procedures to "access, share, compile, identify, collaborate among the cleared contract's function elements and report relevant information covered by the 13 adjudicative guidelines that may be indicative of potential or actual insider threat; deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information and to mitigate risk of an insider threat" **(ISL 2016-02 1-202a)**

Best Practice

In parallel to writing a plan, an assessment should be completed to determine gaps between requirements and business processes
At a minimum, your insider threat plan should detail:

Purpose: Why are you creating this Insider Threat Program?
Scope: Who is required to adhere to this program?
Roles and Responsibilities of Insider Threat Program Personnel

For Non-Possessing, minimum requirement would be Education and Reporting Procedures

Additional Topics to include:

- How do you gather information across your organization?
  - Think about: How are you handling reporting?
  - Think about: How are you keeping records?
- Identify how you measure your program and ensure enforcement
  - Do you have documented policies and procedures?
  - Think about: Graduated security violation plan (NISPOM req)

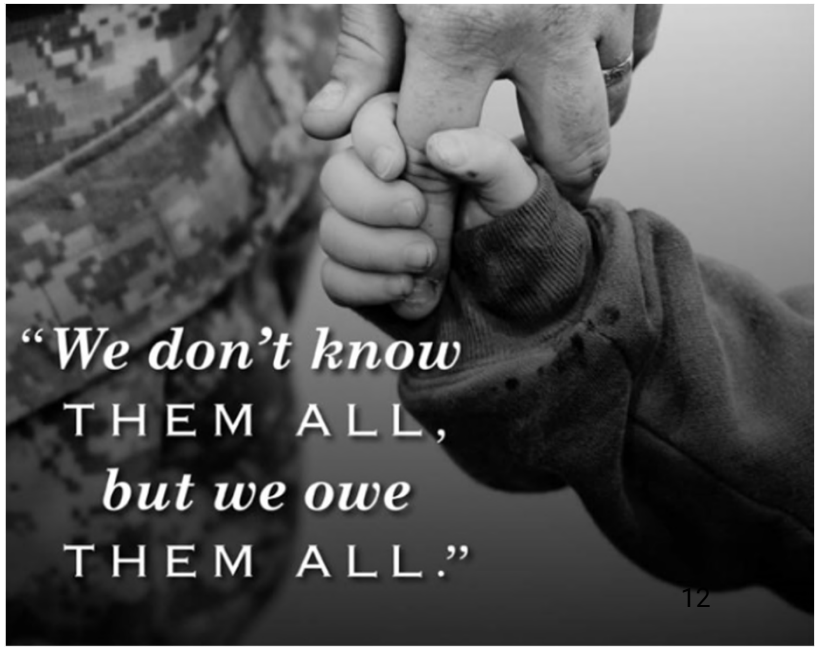
Leading the Insider Threat Program

Best practice

- Insider Threat is a team sport! Include Cross functional partners (HR, IT/Cyber, Management)
- Make program larger than NISP requirements
- Demonstrate effectiveness e.g. identifying behaviors captured by program
- Demonstrate sharing of data and trends
- Focus on National protection of secrets
- Don't make the program punitive

  Stress Employee Assistance Program (EAP)

  “It’s not about turning people in, it’s about turning people around”



The Basics - Training

NISPOM & ISL Requirement

ITPSO, Working Group & Program Personnel

- CI, security fundamentals, legal issues
- Procedures for conducting insider threat response actions
- Applicable laws, regulations regarding gathering, integration, retention, safeguarding and use of records and data including the consequences of misuse of such information
- Applicable legal, civil liberties and privacy policies

Available CDSE Training

- Establishing an Insider Threat Program for your Organization (CI12216)
- Insider Threat Awareness Course (INT101.16)

Cleared Personnel

- Current and potential threats in the work and personal environment
- Importance of detecting potential insider threats by cleared employees and report suspicious activity to the insider threat program designee
- Methodologies of adversaries to recruit trusted insiders and collect classified information, within an Information System
- Indicators of insider threat behavior, procedures to report such behavior
- Counterintelligence and security reporting requirements

Available CDSE Training

- Insider Threat Awareness Course (INT101.16)

Best Practice - Training

Course Number	Course Name	Duration (mins)	Target Audience	Program Maturity	Value to Program	Content Effectiveness	Overall ROI (Duration X Effectiveness)	NCMS Recommended Frequency
INT101.16	Insider Threat Awareness	30	General	Program Establishment	Need to Know	High	High	Annually
CDSE Insider Threat Catalog	Active Shooter Awareness	12	General	Program Establishment	Nice to Know	High	High	As Needed
INT240.16	Insider Threat Basic HUB Operations	60	ITPSO/Program Managers	Program Establishment	Need to Know	High	High	As Needed

In 2020, The NCMS Insider Threat Subcommittee developed a whitepaper and matrix tool that can help to identify free CDSE training that meets the needs of your program.

- Leverage to tool, sorting by:
  - Available Training minutes
  - Target Audience
  - Your Program Maturity Level
  - Value to the Program
  - Content Effectiveness
  - Overall Return on Time Investment
  - Recommended Training Frequency

To find the tool, go to the NCMS Resource Library, Insider Threat Resources, **Evaluation of CDSE Insider Threat Products Matrix Tool.**

Self Inspections & Assessments

DSS Self-Inspection Handbook, May 2016 - Section "Y" Insider Threat

- Appointment "Name of Senior Official In Writing" (Pg. 61)
- Insider Threat Plan (ITP) developed, implemented, endorsed by ITPSO (Pg.62)
- Self-Certification of Written Program Plan
- Written policy, guidelines, procedures (Pg.62, 63)
- No plan – milestones/timelines (Pg. 62)
- Who conducts , who manages reviews, how often? (Pg. 63)
- Process to gather / integrate/ response (Pg. 63)
- Policy and process to ensure timely response, how data is managed (Pg. 63)
- Training – ITPSO, ITP-program personnel (Pg. 64)

Best Practice - Assessments

- **Governance**
  -Do you understand what you are protecting? (Risk Tolerance)
  -How does your organization share information?
  -Do you have documented policies and processes? Are they consistently followed?
- **Training & Awareness**
  -Ensure consistency
  -Consider Role based training (people managers)
  -Workplace Violence or Situational Awareness
- **People Management**
  - Background Investigation Process
  - Continuous Vetting after employment
  - 3rd party vendor & Termination Processes
- **Technical Controls**
  - Provides data to demonstrate operation but not essential for all companies

Preparing for a Continuous Monitoring Engagement (CME)

Example 1

Western Region RFI

1. NISS Facility Profile Update Request
2. Contracts List (template attached)
3. Consultant Security Agreements(if applicable; if company has cleared consultants) N/A
4. Self-Inspection Senior Management Official (SMO) Endorsed Certification (upload in NISS)
5. Security Violation Reports since the last ESVA
6. Suspicious Contact Reports to the CISA since the last ESVA
7. ATO Information and Classified IS List (if applicable)
8. FSO, ISSO, ISSM, ITSPO and ITPSO Working Group Training certificates

Also provided the Insider Threat Plan and answers to questions regarding company cyber posture

Example 2

Northern Region RFI

1. A copy of the facility's Insider Threat Program
2. Consultant Security Agreements (if applicable)
3. Training completion Certificate for FSO required training and ITPSO required training.
4. All current DD254s
5. Last Self-Inspection reported in NISS (ensure the SMO endorsed certification has been completed and uploaded within the NISS self-inspection tab)
6. Security Violation Reports not previously submitted
7. Listing of authorized IS (if applicable)

The Basics - Communication

Overall Strategic Importance

- The role of the ITPSO is crucial in how your insider threat plan and program is communicated to the audience
- Strategic and tactical understanding of the entire program lifecycle
- Effective communication – know your milestones and main points to communicate and what expectations are to your insider threat plan personnel members in the various functions (legal, IT, HR, etc.)

Communications Will Vary By Group

- ITPSO to direct supervision
- ITPSO to Executive Management
- ITPSO to Insider Threat Working Group (many of whom could be un-cleared)
- ITPSO to Impacted or Cleared Employees

Building credibility, trust, and management support through positive communication

- Is your program a “Big Brother”operation?
- Is your program an extension of the EAP?
- Is your program strictly a DLP operation?

The Basics - Reporting

Insider Threat Reporting Requirements

NISPOM and ISL Requirements

Contractors must report relevant and credible information coming to their attention regarding cleared employees (ISL 2016-02, 1-300)

- Reporting should include information indicative of a potential or actual insider threat that is covered by any of the 13 adjudicative guidelines OR when information constitutes adverse information (ISL 2016-02, 1-300)

- No distinction between possessing and non-possessing facilities insider threat reporting requirements!

- That being said – what does a non-possessing facility do for reporting as they have no classified material at their site?

- Work with hosts, US Gov't facilities, prime contractors to get information regarding your cleared-off site personnel, long-term visitors, VGSA personnel

Best Practice

Critical to demonstrate to DCSA effectiveness of the program

- Show a direct link to the Insider Threat program and investigations
- Not every company is going to be able to report Insider Threat include disciplinary actions

- Create a simple secure database to capture internal reports from cross functional partners or within the InT program

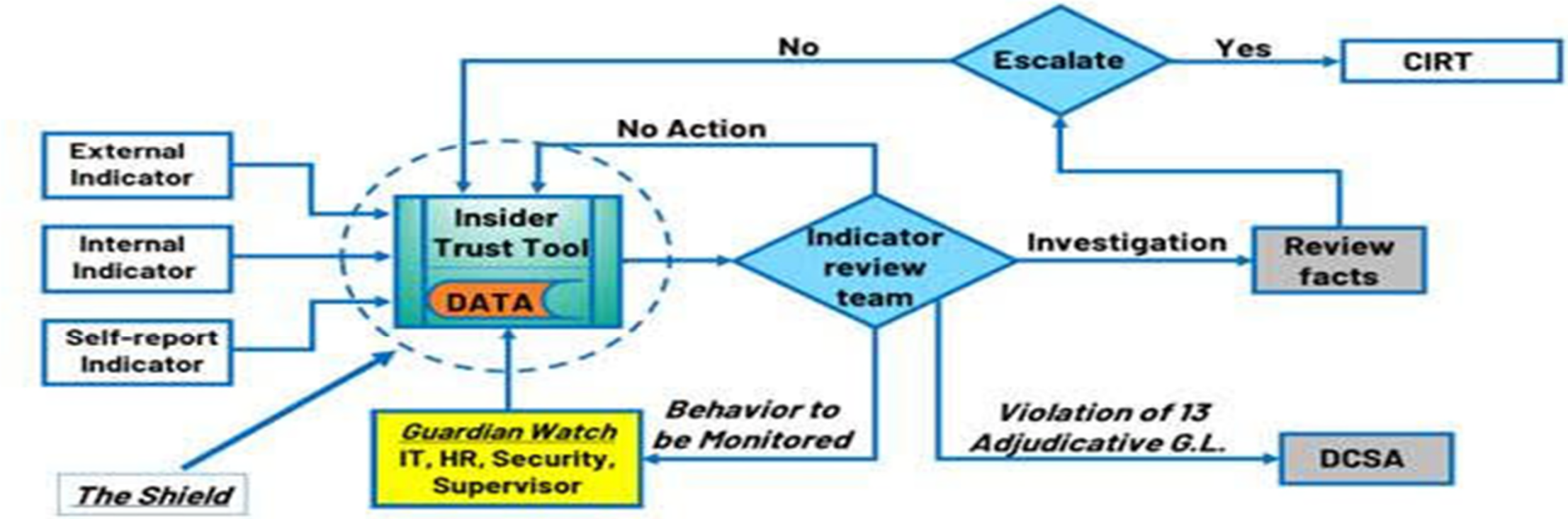
Think about:

Include uncleared people as part of the insider Threat program

Turn your incidents and/or alerts into training opportunities

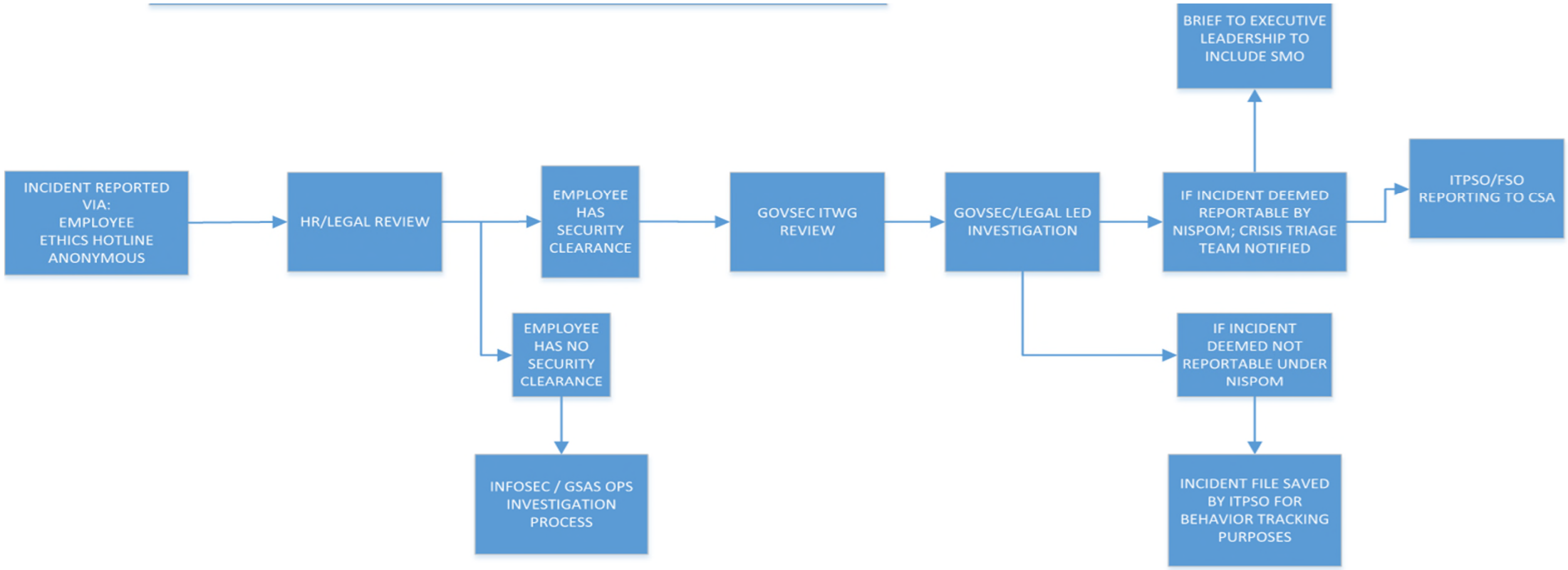
Incident Response

Example 1



Incident Response

Example 2



Metrics

Recommendation– clearly define your metric(s) based upon factual data you can obtain and establish the metrics targets or goals based upon your own organizational requirements and inputs

- # of insider threat referrals per time period (week/month/quarter/year)
  - # of insider threat by referral/source (employee, IT system, 3rd party, hotline, etc.)
  - # of insider threat by type (policy violation, misuse of IT, loss of IP, etc.)
  - # of insider threat referrals converted to cases (or matters to be investigated)
- Insider Threat Incident by Use Case (or Adj. Guideline)
- Hours spent on insider threat matters
- Dollars spent on insider threat matters (salary, capital, type)
- Mean Time to Close Insider Threat portion of investigation
- Mean Time to Respond to Incident
- # of data downloaded/stolen/mishandled, etc.
- Types of data downloaded/stolen/mishandled, etc.
- # of insider threat matters – unverified (time, source, type)
- # of insider threat matters – verified (time, source, type)
- # of matters resulting in re-training, discipline, re-assignment, termination of clearance/access, termination of employment, legal action
- # matters resulting in referral to LEOs/CI entities/Prosecutions
- damage to activity / program / company proprietary information / IP / reputation or brand (estimates)
- $$ Outside Counsel Engagement

Training Resources

Public Resources

DCSA: NISPOM / ISL / CDSE
DCSA: ISR, ISSP, FCIS
US Government Customers (GCAs)
Federal Bureau of Investigations
Infragard, Counterintelligence (Economic Espionage
Cyber Crime, Intellectual Property Theft/Piracy
Non-Customer Public Sector Agencies insider threat programs, LEOs
DHS, US - CERT
Carnegie Mellon Software Engineering Institute

Private Resources

Prime and Subcontractors
NCMS National Insider Threat Subcommittee Members
NCMS Insider Threat Resource Library
NCMS Speakers Database
NCMS Local Chapters / Membership
Non-NCMS: with apologies to NCMS…
…Industry Associations (NDIA/AIA, TriSAC)
…Software Companies - white papers:
"insider threat, big data, predictive analytics, user-behavioral analytics"

Training Resources

CDSE Insider Threat Catalog https://www.cdse.edu/catalog/insider-threat.html

Baseline Insider Threat Training from CDSE

- Insider Threat Awareness INT101.16
- Establishing an Insider Threat Program INT122.16

- National Insider Threat Task Force Maturity Framework
  - https://www.dni.gov/files/NCSC/documents/features/NITTF_MaturityFramework_web.pdf
- Insider Threat Toolkit: Policy/Legal, Reporting, Establishing a Program, Cyber Insider Threat, and Vigilance Tabs
  - **Case Studies, Curricula, eLearning Courses**
  - **Job Aids, Security Awareness Games, Security Awareness Posters**
  - **Security Shorts, Security Training Videos, Security Tool Kits, Webinars**

Resources

The Insider Threat Subcommittee is actively updating these Brown Bags and will start sharing them via NCMS Live Sessions in the Summer of 2021 through Winter 2022!

NCMS Resource Library, Insider Threat Resources: https://classmgmt.com/library.php?c=INSIDER

- April 26, 2017 Brown Bag Presentation – Insider Threat Beyond the Baseline – Presentation & Q/A

  https://classmgmt.com/brown_bags.php

- May 2017 **Insider Threat Program Subcommittee Resource Call Slides & Q/A**

  5/25/17 – **Insider Threat Training**

- June 2017 NCMS National Seminar – Insider Threat Panel Presentation
  Small, Medium, Large facilities' programs, and data from DSS

- July 2017 **Insider Threat Resource Call Sides & Q / A Document**

  7/11/17, 7/21/17 – Non-Possessing Facilities

- August 2017 **Insider Threat Resource Call Slides & Q/A Document**
  8/10/17, 8/14/17 - Self Inspection & Assessment

- September 2017 **Insider Threat Resource Call Slides & Q/A Document (Includes Current/Best Practices via attendees)**

  9/21/17 - **Communications**

- October **Insider Threat Resource Call Slides & Q/A Document (Includes Current/Best Practices via attendees)**
  10/26/17, 11/2/17 - **Metrics & Performance Measurements**

Contact Information

Wailohia Woolsey
wwoolsey@paloaltonetworks.com

Paul Fitzpatrick
Paul.Fitzpatrick@mrcy.com

Insider Threat Subcommittee via NCMS website