Executing an Effective Insider Threat Program from a Practitioners Perspective

Leonard Moss, Jr., CPP®, ISP®, CHS-V
Senior Vice President, Corporate Security, Facilities & Real Estate
Chief Security Officer & Insider Threat Program Senior Official
Abstract: Insider Threat Program – A Practitioners Approach to Effective Implementation

- Governments and Companies increasingly affected by insider threats, resulting in millions of dollars of stolen IP, loss of classified information and other critical assets to include loss of life.
- The US Government now mandates that all of its contractors implement an effective Insider Threat Program
- This presentation will share the approach that was implemented by one practitioner that incorporates industry best practices and has been evaluated as EXCEPTIONAL!
- We will share our method which exceeds NISPOM Conforming Change 2 requirements and incorporates a holistic and full spectrum approach to prevent, monitor, detect, respond, investigate & mitigate insider threats
- We will also share industry best practices that we have implemented
Objectives

• Obtain awareness of the insider threat issue from a Practitioners Perspective

• Become familiar with types of insider threats, motivations and behaviors of insiders

• Know how to prevent, detect, respond to, and report insider threats

• Gain knowledge on insider threat best practices and countermeasures

• Understand roles and responsibilities of an Insider Threat Program Advisory Board Member

• Fulfill NISPOM Conforming Change 2 requirements & Beyond
Module 1: Defining Insider Threat & Obtaining Senior Executive Buy-In

Module 2: Overview of Insider Threat in U.S. Government

Module 3: Prevention and Detection

Module 4: Roles and Responsibilities
# Insider Threat – Government vs. Private Industry

<table>
<thead>
<tr>
<th>Government</th>
<th>Private Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets of value: Classified Information; Personally Identifiable Information (PII); Controlled Unclassified Information (CUI)</td>
<td>Trade secrets, R&amp;D, IP, Source Code, Business Strategy, Blueprints, Financial Information, Customer Information, PII</td>
</tr>
<tr>
<td>Technology: Stand-alone, LAN’s &amp; WAN’s classified networks vulnerable to internal and external threats</td>
<td>Networks vulnerable to internal and external threats</td>
</tr>
<tr>
<td>Personnel: Classified environments receive security training and practice need-to-know</td>
<td>Security awareness training is sporadic and need-to-know is not a well known or practiced concept</td>
</tr>
<tr>
<td>Damage: Release of classified information can cause exceptionally grave damage to national security or loss of life</td>
<td>Loss of R&amp;D, IP, revenue, jobs and competitive advantage; reputational damage</td>
</tr>
</tbody>
</table>
MODULE 1: DEFINING INSIDER THREAT
Insider Threat Definitions

**DCAS**
“The threat that an insider will use his or her access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or the loss or degradation of government, company, contract or program information, resources, or capabilities.”

**CERT**
“Insider threat is the potential for a current or former employee, contractor, or business partner to accidentally or maliciously misuse their trusted access to harm the organization’s employees, customers, assets, reputation or interests.”
Types of Insider Activities

1. **Espionage** – Act of secretly gathering information about a foreign government or a competing industry, with the purpose of providing financial or strategic advantage to one’s own government or corporation

2. **Sabotage** – Directing specific harm at an organization or individual(s)

3. **Theft** – Use of IT/authorized access to steal intellectual property and material items from the organization

4. **Fraud** – Unauthorized modification, addition, or deletion of an organization’s data for personal gain, or theft of information leading to fraud (identify theft, credit card fraud)

5. **Workplace Violence** – Use of violence or threats of violence to influence others and impact the health and safety of the workforce

6. **Unintentional/Accidental** – Insider whose actions or lack of action(s) without malicious intent causes harm or possibility of harm
MODULE 2: U.S. GOVERNMENT INITIATIVES
U.S. Government Initiatives

Threat Task Force (NITTF) whose mission is focused on preventing, determining and detecting the compromise of classified information.

**National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs:** Issued in 2012 to require all Executive agencies that access classified information to establish insider threat detection programs.

**Department of Defense Directive (DoDD) 5205.16:** Issued in 2014 to establish policy and assign responsibilities within DoD to develop and maintain an insider threat program, to include training and awareness initiatives.

**NISPOM Change 2 and ISL 2106-02:** Issued May 2016 to require all cleared contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats.
NISPOM Conforming Change 2

Five General Areas

1. **Insider Threat Program** ✓
   - Gather, integrate and report
   - Designate an Insider Threat Program Senior Official (ITPSO)
   - Addresses requirements for all cleared facilities

2. **Security Reviews: Self-Inspections** ✓
   - DSS handbook
   - Annual requirement

3. **Reporting Requirements** ✓
   - Establish internal procedures
   - Prior to being granted access to classified info, employees will receive security briefing that includes reporting obligations
   - 13 personnel security adjudicative guidelines

4. **Insider Threat Training** ✓
   - Those with insider threat program management responsibilities
   - Cleared employees

5. **Protection Measures** ✓
   - Monitor user activity on classified IS in order to detect activity indicative of insider threat behavior
Enhancements: Beyond NISPOM

1. Incorporates critical assets and proprietary information in addition to just classified; enforces security beyond the classified environment

2. Stand-up of an Insider Threat Program Advisory Board (ITPAB)
   - Wider representation for better cross-collaboration corporate wide
   - Governance and set procedures
   - Led by ITPSO
   - Responsible for individual business area and corporate-wide

3. Self-Inspections / Vulnerability Assessments go beyond DCSA (DSS) handbook
   - Includes industry standards and best practices (CERT, NIST, SANS)
   - Creation of capability workbooks
   - Wider scope: classified and critical assets

4. Insider Threat Training further reaching and wider scope
   - Protection of critical assets and all that is of value to a company
   - Employee wide training, not just cleared employees
   - Training schedule

5. Protection Measures expand beyond classified systems
   - Focus on what is of value
   - Networks, systems and accesses considered to protect critical assets

6. Policy Development
7. Change Management
MODULE 3: PREVENTION AND DETECTION
Potential Behavioral Red-Flags (That May Require Closer Review)

- Depression
- Exhibits addictive traits (drugs, alcohol, gambling)
- Financial trouble
- Prior and recent disciplinary issues
- Sudden reversal of financial situation, unexplained affluence, repayment of debts/loans
- Threats to people or property
- Unusual working hours
- Out of scope work requests
- Attempted access to restricted or unauthorized data/spaces
- Questionable downloads; large print jobs, forwarding data to personal emails
- Solicitation of information or interest in matters outside of work scope
- Unusual remote access of computer network

*Patterns are critical.*
Potential Espionage Red-Flags (That May Require Closer Review)

- Repeated security violations; disregard for security rules and procedures
- Unexplained affluence
- Engaging in suspicious personal contacts
- Failure to report overseas travel or foreign contact; short trips to foreign countries
- Seeking higher clearance or greater access outside of job scope
- Attempting to enter unauthorized areas
- Inconsistent work hours from job duties; insistence on working in private, during weekends or off hours
- Concerned they are being investigated
- Overwhelmed by life crises or career disappointments
Prevention and Countermeasures
Protecting Your Organization: Where Do You Begin?

1. Core: Determine critical assets (classified and unclassified)
2. Identify personnel and systems that touch critical assets
3. Identify vulnerabilities and risks
4. Consider personnel, processes, and technology
5. Incorporate full spectrum of business components
   - Data Owners
   - Human Resources
   - Information Technology
   - Physical Security
   - Legal/Contracts
   - Trusted Business Partners / Third Parties
6. Internal and external business operations
7. Build for malicious and unintentional threats
8. Focus on prevention, detection, and response to threats
9. Develop governance structure and policy
10. Include organizational cross-collaboration and information integration
11. Cover full employee lifecycle
Industry Standards

- Executive Order 13587
- Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs
- DSS - NISPOM
- CERT
- National Insider Threat Task Force (NITTF)
- International Organization for Standardization (ISO)
- National Institute for Standards and Technology (NIST)
- National Infrastructure Advisory Council (NIAC)
- Federal Information Security Management Act (FISMA)
- SANS Institute
- Intelligence and National Security Alliance (INSA)
- Federal Bureau of Investigation (FBI)
- National Counterintelligence and Security Center (NCSC)
- Armed Forces Communication and Electronics Association (AFCEA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Securities Industry and Financial Markets Association (SIFMA)
- Health Insurance Portability and Accountability Act (HIPAA)
Best Practices in Countering Insider Threat

1. Clearly document and consistently enforce policies and controls
2. Incorporate insider threat awareness into periodic security training for all employees
3. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior
4. Anticipate and manage negative issues in the work environment
5. Know your assets
6. Implement strict password and account management policies and practices
7. Enforce separation of duties and least privilege
8. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities
9. Institute stringent access controls and monitoring policies on privileged users; privileged user access management
10. Institutionalize system change controls
11. Develop a comprehensive employee termination procedure
12. Implement secure backup and recovery processes
13. Develop a formalized insider threat program
14. Establish a baseline of normal network device behavior
15. Be especially vigilant regarding social media
16. Close the doors to unauthorized data exfiltration

Best Practices in Countering Insider Threat

1. Human Resources – Best Practices Recommendations

2. Legal – Best Practices Recommendations

3. Trusted Business Partners/Third Parties: The Forgotten Weak Link

4. Data Owners – Best Practices Recommendations

5. Information Technology – Best Practices Recommendations

6. Privacy Best Practices
Detection: Connecting the Dots

Duty of Insider Threat Program Advisory Board
- Forum to:
  - Cross-collaborate across business areas
  - Integrate and share information
  - Discuss behavioral indicators
  - Raise suspicious activity
  - Collect and analyze data
  - Implement new controls
  - Respond to incidents
- Incorporate:
  - All business areas
  - Human factor, processes and technology
  - Full employee lifecycle
- Oversight:
  - Inspections
  - Lessons learned
Detection: Monitoring

Monitoring employees’ activities may alert companies to those who are abusing systems and network access as well as physical security accesses which may be potential insider threats.

Types
• Tracking employee behaviors and activities - physical
• Monitoring technology – systems, networks (file, print, search activities)
  – Example: Failed attempts to gain access to a critical data asset by an employee without a need-to-know (includes physical and virtual).

Privacy and Civil Liberties
• Employees have no legitimate expectation of privacy at work while using company media systems; therefore, all activities on company-owned systems can be monitored, including email, phone, and web history
• Employees should be required to sign a “Consent to Monitoring Agreement”
  – This should be part of insider threat training; a reminder that their work-related activities are monitored, and that they should have very little expectation of privacy
  – All systems should also have a “Consent to Monitoring” warning at login
• BYOD: Current Legal Gray Area
  – Easily solved with a BYOD policy, requiring employee signature and acknowledgement of monitoring
  – Mobile Device Management Software (MDM) can enable employer-triggered remote wipe and location tracking
Privacy Considerations

As insider threat programs focus on people, this can raise several privacy considerations.

• US federal and state statutes protect personnel files, HR info, healthcare and media data and certain intercepted electronic communications
• Data on foreign employees or organizations with international offices may be subject to foreign data privacy protections (i.e., EU Privacy Directive)
• Transparency regarding business practices that result in use and disclosure of employee information (employee consent and notice: user agreement, login banners)
• Protection mechanisms must be established to address privacy considerations when handling, processing and storing data
• Those handling sensitive data need to be well trained and controls in place to ensure privileges aren’t abused
• Indiscriminate or intrusive monitoring systems can have negative business and legal implications
• Cultural and religious considerations
MODULE 4: ROLES AND RESPONSIBILITIES
Why You?

A successful insider threat program requires cross-collaboration and data integration throughout the organization with involvement from various business areas.

Critical business areas to insider threat include:
- IT
- Ethics
- R&D
- HR
- Contracts
- C-Suite
- Security/CI
- Supply Chain
- BD
- Legal
- Finance
- Operations

You represent the core business areas for a successful Insider Threat Program!

Representative of the human element portion of an Insider Threat Program.
Insider Threat Program Advisory Board

Purpose

- Implement NISPOM Conforming Change 2 requirements
- Detect insider threat vulnerabilities across the organization, both in classified and unclassified environments, determine gaps, and bolster insider threat security posture
- Mitigate insider threat risks in the organization and include a scope that encompasses the entire lifecycle of the employee
- Develop and implement insider threat policies
- Prevent, detect and respond to insider threat activity
- Protect the organization from malicious and unintentional insider threat activities while mitigating insider threat and legal risk
Components of Insider Threat Program

- Critical Asset Identification
- Vulnerability Assessment
- ITP Advisory Board
- Policy Development
- Training and Awareness
- IT Solutions

Change Management

- Security
- HR
- IT
- Legal
- NSP
- Finance
- Ethics
- BD
- Operations
- Contracts
- Supply Chain
- Cont. Improvement

- Enterprise wide participation
- Cross-collaboration organization wide
- Central management of program, data
- Data collection and integration
- Human and technology analysis
- Report, respond and escalate
Insider Threat Program – Components

*Source: Robert L. Bean, COBHAM*
Appendix

Our Program’s Successful Approach &
Defense Counterintelligence & Security Agency (DCSA) Tools
Agenda

• NISPOM Change 2 Requirements
• Implemented Enhancements beyond NISPOM
• Insider Threat Program Advisory Board Concept
• Education and Awareness
• Policy Development
• Self-Inspections / Vulnerability Assessments
• Development of Capability Notebooks
• Change Management and Communications Strategy
• Cross-Organizational Collaboration
• Mitigation Plan Status
• Examples of Best Practices
Insider Threat Program Advisory Board

- Led by Insider Threat Program Senior Officer – Representation from critical and relevant business areas
  - Security, HR, IT, Legal, Finance, Procurement/Supply Chain, Operations, Business Development, Contracts, Ethics & Trade Compliance
- Oversee Insider Threat Program and insider threat activity
- Prevent, monitor, detect, report, respond
- Conduct/Support self-inspections
- Develop policies and procedures and ensure they are relevant and updated
- Deliver messages to their business areas
- On-going Training
- Meet once a month or ad-hoc as needed

- ITPAB Appointment – Leadership By-In
Education and Awareness

Training for Insider Threat Program Advisory Board

• Instructor led course – 2 days
• Topic areas include:
  – Types of insider threat, motivations and behaviors of insiders
  – CI and security fundamentals to include countermeasures
  – Introduction to roles and responsibilities
  – Exposure to legal issues, privacy and civil liberties
  – Insider threat program best practices
• Future iterations

Awareness Training for Employees

• Online course
• Topic areas include:
  – Importance of detecting potential insider threats and how to report them
  – Types of insider threat, motivations and behaviors of insiders
  – Methodologies used by adversaries
  – How you’re a target and what is of value to adversaries

• Annual Requirement for all Employees
Policy Development

- Led by ITPSO and ITPAB with assistance from consultants
- Provided ITPAB with best practices and industry standards as foundation
- Commence development in September 2015; continued development through October and finalizing by end of October
- Publicized relevant policies and procedures to workforce
- Program promulgated by CEO
- Published and Communicated to all employees
Self-Inspections / Internal Vulnerability Assessments

• Based on internally developed capability workbooks

• Develop checklist of questions/ evidence

• Incorporates NISPOM recommendations from handbook as well as industry standards
Capability Workbooks

• Based on industry standards and best practices
• Workbook per critical area
• Foundation for vulnerability inspections
• Provide ITPAB guidance
• Baseline for policy development
• Critical Asset Capture
Cybersecurity Regulatory Compliance (2017)

- The October 8, 2015 class deviation to DFARS Clause 252.204-7012 expanded the scope of applicable information, systems and controls
  - Covered Defense Information is broadly defined and includes previous Unclassified Controlled Technical Information (UCTI)
  - Applicable to new bids
  - Mandates subcontractor compliance

- Cyber Security Implications
  - Inclusion of NIST 800-171 increases number of controls to ~170
  - Existing policies may need to be adjusted and new policies will be required
  - Satisfying control objectives requires implementation of additional cyber security related capabilities for Mobile Devices, User Authentication, and Data Loss Prevention

<table>
<thead>
<tr>
<th>DFARS Related Clause Controls</th>
<th>2013 Clause</th>
<th>NFO*</th>
<th>CUI*</th>
<th>Net Diff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>12</td>
<td>1</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Audit &amp; Accountability</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Configuration Mgt.</td>
<td>4</td>
<td>6</td>
<td>13</td>
<td>19</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Identity &amp; Authentication</td>
<td>3</td>
<td>1</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>Incident Response</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Maintenance</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>Media Protection</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Physical &amp; Environmental</td>
<td>3</td>
<td>5</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Program Mgt.</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>System &amp; Comm Protection</td>
<td>7</td>
<td>5</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>System &amp; Info Integrity</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Assessments</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>51</strong></td>
<td><strong>36</strong></td>
<td><strong>73</strong></td>
<td><strong>109</strong></td>
</tr>
</tbody>
</table>

NFO
- EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION

CUI
- THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT
Future State: Path to Reduce Business Risks (2017)

Risk profile will guide cyber security policies and business process changes

<table>
<thead>
<tr>
<th>Likelihood of Incident Scenario</th>
<th>Very Low (Very Unlikely)</th>
<th>Low (Unlikely)</th>
<th>Medium (Possible)</th>
<th>High (Likely)</th>
<th>Very High (Frequent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LEGEND

- Light Blue = Existing Risk
- Dark Blue = Residual Risk After Strategy Implementation

Very High
(Frequent)
High
(Likely)
Medium
(Possible)
Low
(Unlikely)
Very Low
(Very Unlikely)
Cybersecurity Compliance Deficiencies (2017)

1. **Information Asset Management**: Data Loss Prevention (DLP). *Encryption of email ensures email content is not compromised enroute to non-DI recipients.*

2. **Enterprise Mobility Management (EMM)**: We have limited capabilities to protect both company-owned and personally-owned mobile devices (phones, tablets, laptops, etc.), including segmentation of company and personal information.

3. **Multi-Factor (MFA) & Network Access Control (NAC)**: We are exposed to the risks associated with password compromise and the inability to make network access contingent on compliance (trusted device, patched, virus free, AV version, etc.).

4. **Compliance**: Recently released USG Controlled Unclassified Information (CUI) rules have been stipulated in the FAR and non-compliance could potentially reduce competitiveness or disbarment.
Cybersecurity Committee Accomplishments

• DFARS Cybersecurity Impact & Strategy ✓
• Information Asset Management ✓
• Email Encryption ✓
• Enterprise Mobility Management (EMM) ✓
• Multi-Factor Authentication (MFA) ✓
• Compliance ✓
Change Management

- Obtain buy-in from all levels
- Developed change management plan and communications strategy
- From ITPAB to workforce wide communications
- Worked directly with communications department
- Implemented communications plan
- Developed Insider Threat SharePoint Site & Webpage
Phase II

- Capture Lessons learned
- Refine and update
- Launched Phase II self-inspections in subsequent years
- Assess ITPAB meetings and collaboration
- Continue communications plan
Internal SVA

- ITVA Scope: NISPOM CC#2 Annual Requirement & Critical Assets
- Develop Assessment Schedule, Coordinate and Communicate in Advance
  - ITPAB & FSO’s support
- Entrance & Exit Briefing with Local Executives/Leaders
- Diversified Pool Of Candidates Interviewed – ITPAB Members, Executives, Non-management Professionals (Exempt And Non-exempt)
- Questions: Critical Assets Captured, Insider Threat Mitigation Best Practices
- Raise Awareness And Educate
- Mindset Shift
- Feedback
- Comprehensive Assessment & Report (SLT & ITPAB)
- Final Report Divided Into 8 Sections & 7 Appendixes
  - Introduction, Executive Summary, Key Findings, Compliance with NISPOM, Insider Threat Vulnerabilities, Observed Best Practices, Risk Mitigation Plan/Next Steps, Conclusion
  - Findings categorized as either: Technology, People, Data or Security
Do You Think Your Company’s Crown Jewels Are Safe?
Executive Summary

• Key Findings: The Good News!
  – We are Effectively Protecting Classified Information
  – Our Program Exceeds NISPOM Requirements – This Helped Us Earn Superior Ratings!
  – We Executed Best Practices
    • Establishment of ITPAB (Entire Org Represented)
    • Policies & Standards Implemented
    • Education & Awareness Program for all Employees
    • Senior Leadership Support
    • Scope Includes Classified, CUI & Proprietary
    • Identification of all Critical Assets
    • Comprehensive Self-Assessment
    • Independent & Objective Assessment of Program
    • Employee Engagement & Significant Increase in Reporting
Executive Summary

- **Key Findings: Best Practices & Vulnerabilities/Opportunities**
  - The Team Identified Numerous Best Practices Observed In The Following Categories:
    - Data
    - People
    - Security
    - Technology
  - The Full List of all findings Best Practices and Opportunities were contained in a comprehensive report provided to Senior Leadership
- We used an adversary’s approach to the assessment & our leadership was receptive to improvement
- ITPSO briefed ITPAB & SLT to obtain buy-in & resources for mitigation plan. A picture is worth a thousand words!
Photos!

“A Picture is Worth A Thousand Words”
Risk Mitigation Plan & Next Steps

- Our Self Report Identified **Vulnerabilities**, Location, Associated Risk And Recommendations To Mitigate Each

- Vulnerabilities are segmented by the following categories:
  - Data
  - People
  - Security
  - Technology

- ITPSO Assigned The Logical ITPAB Representative To Lead Segment Mitigation
Accomplishments & Next Steps

- Program Fully Executed & Exceeded NISPOM Requirements
- The Insider Threat Program has been a great benefit in Enhancing Our Security Posture
- Annual Insider Threat & CUI rolled out for 2nd Year-100% completed
- We have received, adjudicated and proactively mitigated actionable actual Insider Threat Cases
- With Senior Leadership Concurrence Worked With The ITPAB to Implement Mitigation Plan
- Most Mitigation Measures Were at Minimal Cost
- 100% of all Vulnerabilities have been Mitigated
- 2019 Insider SVA – Scheduled
- CPI our Program - Ongoing
Where do I go for Information on Establishing a Program?
Defense Counterintelligence and Security Agency (DCSA)

www.dss.mil

www.cdse.edu
One Stop For Insider Threat Information

WWW.DSS.MIL
Insider Threat Job Aid for Industry
Insider Threat Job Aid for Industry

Center for Development of Security Excellence - Insider Threat Job Aid for Industry

Practices:
- In line with the training topics designated for Insider Threat Program personnel, it is a good idea to keep up-to-date on topics related to counterintelligence, security and defensive security fundamentals, laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data (including the consequences of misuse of such information) and applicable legal, civil liberties, and privacy policies. Awareness of legal and policy changes, both internal to your company and at the state, local, and federal level, will ensure that all elements of the program run smoothly.
- When establishing procedures for conducting Insider Threat response actions, look to existing company policy and industry standards.

Training and Resources:
- eLearning Course: Establishing an Insider Threat Program for Your Organization G123.16

Insider Threat Toolkit Tab: Establishing a Program

http://www.ciose.org/catalog/insider-threat.html
Questions

????