DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
NISP MISSION PERFORMANCE DIVISION
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

December 9, 2025

Mr. Christopher Stolkey
Chair
NISP Policy Advisory Committee
Insider Threat Working Group

Dear Mr. Stolkey:

This letter pertains to the request from the National Industrial Security Program (NISP) Policy Advisory Committee (NISPPAC) Insider Threat Working Group to the DCSA Industrial Security Mission Headquarters for review and validation of the submitted insider threat training for program personnel.

DCSA NISP Mission Performance Division has reviewed the NISPPAC insider threat training for program personnel, dated December 9, 2025, and validated that it includes the minimum requirements of 32 CFR Part 117, "National Industrial Security Program Operating Manual (NISPOM)," §117.12 (g)(1).

This validation pertains to the enclosed training slides in their current state only. NISPPAC may share a copy of this validation letter with the enclosed training slides throughout the industrial security community for use. Any edits or modifications to the enclosed slides will require a separate review and validation by DCSA.

Should you require further assistance regarding this matter, please contact me at (571) 969-0476 or misty.l.crabtree.civ@mail.mil.

Sincerely,

CRABTREE.MISTY.LYNN.1
239844266

Digitally signed by
CRABTREE.MISTY.LYNN.1239844266
Date: 2025.12.09 16:20:25 -05'00'

MISTY L. CRABTREE
Senior Action Officer, Industrial Security

Enclosure: Training Slides

cc: NISPPAC Industry Spokesperson

NISPPAC Insider Threat Training for Program Personnel

12/9/2025

Training Objectives

- **Understand Insider Threats** – Define insider threats and recognize their impact on national security and organizations.
- **Apply Counterintelligence & Security Fundamentals** – Integrate CI awareness into daily responsibilities and security programs.
- **Identify and Report Threats** – Recognize common methods of operation, vulnerable groups, and reporting requirements.
- **Implement Countermeasures** – Apply strategies to reduce vulnerabilities, protect assets, and mitigate risks.
- **Comply with Laws & Regulations** – Understand applicable policies, privacy protections, and civil liberties considerations.
- **Support an Effective Insider Threat Program** – Contribute to a culture of vigilance, resilience, and shared responsibility.

Background

Contractors must ensure program personnel assigned insider threat program responsibilities complete training consistent with applicable DCSA-provided guidance.

The term "program personnel" refers to those individuals who manage the insider threat program, including the Insider Threat Program Senior Official (ITPSO).

The ITPSO is responsible for identifying specific individuals within their organization who are considered program personnel and therefore subject to these training requirements.

Requirements

- **The NISPOM, section 117.12(g)(1), requires “program personnel” to be trained in the following areas:**
  - CI and security fundamentals
  - Procedures for conducting insider threat response actions
  - Applicable laws and regulations regarding the 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 and requirements applicable to insider threat programs
- **This training is required to be completed one time**
- **The following four sections of this training cover the requirements above**

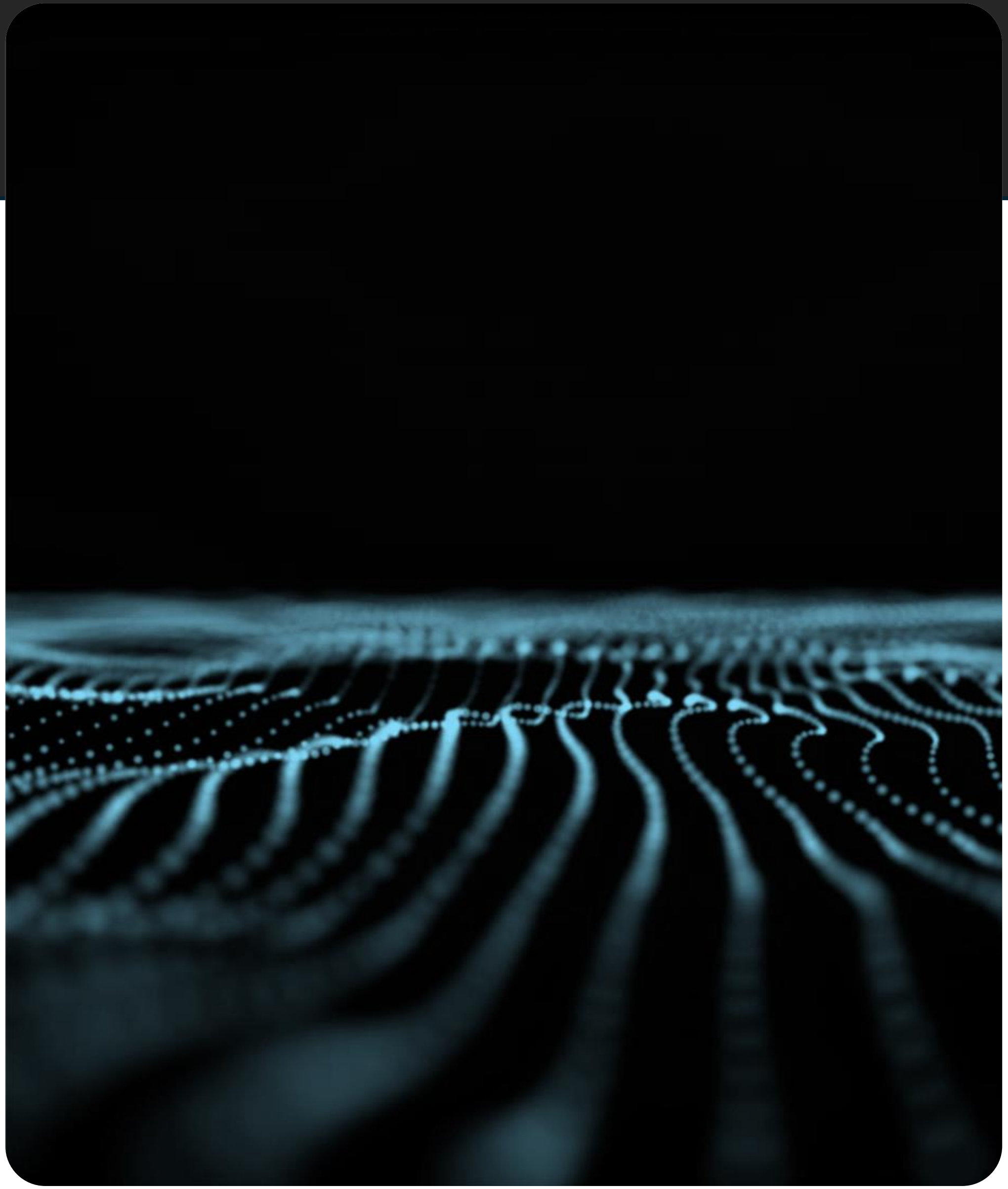
What are Insider Threats?

DEFINITION:

Insider threats refer to the risk of harm to an organization caused by individuals within the organization, such as employees, contractors, or business partners.

TYPES:

- **Malicious Insiders**: Individuals who intentionally harm the organization.
- **Complacent:** Individuals who knows the rules and still choose to operate outside of those rules for non-malicious reasons.
- **Negligent Insiders**: Individuals who cause harm through carelessness or non-malicious mistakes



National Threat Policy Minimum Standards

The National Insider Threat Minimum Standards are guidelines established to help federal agencies develop and implement effective insider threat programs. These standards aim to detect, deter, and mitigate insider threats, which are risks posed by individuals with authorized access to an organization's resources who may use that access to harm national security.

Key elements of the National Insider Threat Minimum Standards include:

1. **Program Management and Governance**:
   - Agencies must establish a formal insider threat program with clear policies and dedicated personnel to oversee its implementation and management.
2. **Information Integration and Analysis**:
   - Agencies are required to integrate and analyze data from various sources, such as security clearances, personnel records, and network activity, to identify potential insider threats.
3. **Workforce Training and Awareness**:
   - Training programs must be developed to educate employees about insider threats, recognizing suspicious activities, and understanding reporting procedures.
4. **Monitoring and Auditing**:
   - Continuous monitoring and auditing of user activity on information systems are essential to detect unusual or suspicious behavior that may indicate an insider threat.
5. **Investigation and Response**:
   - Agencies must have procedures in place to investigate and respond to potential insider threats promptly and effectively, ensuring appropriate actions are taken to mitigate any risks.

By adhering to these standards, federal agencies can create robust insider threat programs that protect sensitive information and national security while fostering a culture of security awareness and responsibility among employees.

CI & Security Fundamentals

Protecting Assets

Elements of a Successful Program

A truly effective security program will take into consideration the principles of risk management. These efforts identify your critical assets, determine the threats against them, identify vulnerabilities at your facility that an adversary is likely to exploit, and help find effective countermeasures.

Elements of Successful CI Programs

- Risk-Based Approach to CI
- DCSA Collaboration & Partnership
- Senior Leadership Support
- Employee Awareness
- Strong Cybersecurity Program
- Employee Foreign Travel Program
- Foreign Visitors Program
- Special Access Program (SAP) / Critical Program Information Protection
- Insider Threat Program (ITP)
- Reporting

Counterintelligence Polices & Requirements

- **32 Code of Federal Regulations (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM):** Controls disclosure of classified information by the Federal Government and DOD Agencies to their contractors and establishes safeguards for special classes of information.
- **Industrial Security Letters (ISLs):** Provide information and clarification of existing policy and requirements.
- **Standard Operating Procedures (SOPs):** Instructions for implementing the requirements of the NISPOM.

ISL 2021-02 provides guidance to contractors and covered individuals on the submission of adverse information and the reporting requirements of Security Executive Agent Directive 3, or SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position."

Introduction to CI & Threat Awareness

Counterintelligence (CI): Information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements hereof, foreign organizations or persons, or international terrorist activities.

Security:

- Focuses on establishing standards, adhering to those standards, and fixing weaknesses
- Protect assets and reduces vulnerabilities
- Takes an inside-out perspective, examining the company's activities and assets

+

CI:

- Focuses on identifying, understanding, and countering adversary collection efforts
- Prevents, detects, responds to, and sometimes exploits foreign intelligence entity (FIE) threats
- Takes an outside-in perspective, examining the company from the adversary's perspective

Incorporating CI into your Security Program:

- Identifying & Prioritizing Assets
- Assessing Risk, Threat & Vulnerability
- Sharing Threat Information
- Deploying Security Countermeasures
- Reporting Suspicious Contact(s)
- Establishing an Insider Threat Program (ITP)

Together, Security and CI provide greater understanding of the threats and how to protect your company's operations and assets.

The Role of Analytical Risk Management in Identifying Threats

The ability to protect company information, technology and personnel depends on your ability to understand and identify threats. The analytical risk management process helps security officials manage risk by focusing on assets, identifying threats to them, identifying vulnerabilities, and developing appropriate countermeasures.

IDENTIFYING ASSETS

Assets include (PIEFAOS):

- **P**eople
- **I**nformation
- **E**quipment
- **F**acilities
- **A**ctivities
- **O**perations
- **S**uppliers

IDENTIFYING THREATS

Determine:

- Adversaries of the company & programs
- Who wants to gain access
- Capabilities and intentions of these adversaries

IDENTIFYING VULNERABILITES

Identify Existing Weaknesses in:

- Information Systems
- Policies & Procedures
- Security Practices

ASSESSING RISK

Impact of Loss or Compromise:

- Loss of valuable intellectual property
- Compromise of classified information
- Cancellation of government contracts
- Financial losses
- Damage to company reputation
- Impact on national security

DEVELOPING & APPLYING COUNTERMEASURES

Countermeasures: Devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. *Countermeasures include:*

- Training employees to recognize and report potential threats
- Controlling access to targets
- Detering FIEs from acting
- Degrading the progress of any FIE into or out of the facility
- Responding to any active threat action
- Creating a secure environment
- Designing programs to mitigate possible harm

Identifying Threats

The Defense Counterintelligence & Security Agency (DCSA) releases an annual "Targeting U.S. Technologies" report that outlines the threats facing the industrial base. Increasing your knowledge of the targeted technologies, collection methods, and countermeasure will keep information from falling into the hands of FIEs and other adversaries.

THREATS

- **Threats to your facility are diverse, dynamic, and complex. These threats may arise from people that have legitimate access to your company. This includes company employees, consultants, subcontractors, and custodial personnel.**

TYPES OF THREATS

- **Business Competitors**: Companies in the same industry that may use questionable means to gain advantage
- **Criminal Activities:** Persons or groups attempting to exploit security lapses.
- **Insider Threats:** Individuals with authorized access who may harm national security.
- **Foreign Intelligence Entities (FIEs):**
    - State-sponsored intelligence activities
    - Foreign commercial organizations
    - Quasi-governmental organizations (universities, research centers)
    - Individuals
- **Terrorist Organizations:** Groups seeking to disrupt economy, degrade national security, or cause fear.

MOST TARGETED TECHNOLOGIES

Both classified and unclassified technologies are targeted

- Command, Control, Communication, and Computers (C4)
- Software
- Electronics
- Aeronautics Systems
- Services & Other
- Position, Navigation & Time
- Marine Systems
- Energy Systems

GROUPS MOST VULNERABLE TO TARGETING

- Human Resources (HR)
- Information Technology (IT)
- Business Development (BD)
- Research and Development (R&D)
- Manufacturing
- Purchasing
- Facility Management
- Employees Traveling Abroad

Sources of Threat Information

Threat summaries and intelligence reports can provide an overall picture of the threat and are available through many sources.

Government Contracting Activity (GCA): Provides contract-specific threat information and threat assessments that identify what makes a facility a target. Key contacts include Contracting Officer's Representatives (CORs), Security Officers, and Military Department or DCSA CI Special Agents.

DCSA CI Directorate: Publishes annual trend reports summarizing threat reports from cleared contractor facilities, showing trends in targeted technologies and methods used. Classified editions with more detailed information are available to security professionals with appropriate clearance and need-to-know.

Federal Bureau of Investigation (FBI): Has primary responsibility for CI investigations within the U.S. and partners with government entities, academic institutions, and the private sector to share information on espionage, CI, counterterrorism, economic espionage, and cyber/physical infrastructure protection.

Other Federal, State, and Local Agencies:

- Department of Homeland Security (DHS)
- Defense Intelligence Agency (DIA)
- Department of State Bureau of Diplomatic Security
- National Counterintelligence and Security Center (NCSC)
- The Interagency Operations Security (OPSEC) Support Staff
- State and local law enforcement agencies

Open Sources

While government sources are preferred, open sources can provide valuable threat information through:

- News media
- Internet resources
- Books and publications
- Publications from other companies
- U.S. and foreign government publications and websites

Security professionals should work with their Industrial Security Representative (ISR) and CI Special Agent (SA) to identify appropriate sources for their organization's specific needs.

Methods of Operation & Methods of Contact

The United States leads the world in producing critical technologies that are the foundation of our technological, economic, and military advantage. It is crucial that we recognize the threats and protect the critical technologies we develop, and the sensitive and classified information entrusted to us from exploitation by FIEs.

METHODS OF OPERATION (MOs)

Distinct patterns or procedures characteristic of individuals or organizations involved in intelligence activities to include:

- Attempted Acquisition of Technology
- Résumé Submission
- RFI/Solicitation
- Search/Seizure
- Surveillance
- Theft
- Exploitation of:
    - Business Activities
    - Cyber Operations
    - Experts
    - Insider Access
    - Relationships
    - Security Protocols
    - Supply Chain

METHODS OF CONTACT (MCs)

Approaches used by foreign actors to connect with targeted individuals, information, networks, or technology to execute their operations.

- **Requests for Information:** Unsolicited requests often via email
- **Academic Solicitation:** Using students, professors, or researchers as collectors
- **Suspicious Network Activities:** Malware, hacking, phishing
- **Targeting at Conferences/Trade Shows:** Connecting with technical experts
- **Foreign Visits:** Gaining access to facilities and employees
- **Solicitation and Seeking Employment:** Placing foreign personnel in facilities
- **Elicitation and Recruitment:** Developing relationships to extract information

Foreign Travel & Foreign Visit Programs

Foreign Travel Program:
Designed to prepare travelers for potential targeting by FIEs and provide strategies to protect employees and sensitive information when personnel travel internationally.

Pre-Travel Briefings: Increase awareness of:

- Potential targeting
- Personal safety precautions
- Travel safety tips
- Current travel warnings and alerts

Post-Travel Debriefings: Gather information about suspicious contacts or incidents that occurred during travel, covering:

- Countries and dates visited
- Irregularities at ports of entry
- Gifts or provisions received
- Foreign inquiries and requests
- Unexpected or unusual events
- Suspicious foreign contacts

Foreign Visit Program:
Manages the CI risks associated with hosting international visitors at cleared facilities. Foreign visits can result in the loss of technology or information or lay the groundwork for targeting by other means by providing access to facilities and employees.

Pre-Visit Activities:

- May notify DCSA Industrial Security Representative (ISR) or CI agent in advance
- Educate escorts, briefers, and hosts on their responsibilities
- Verify visitors' identities
- Implement Technology Control Plan (TCP)

During Visit Vigilance:

- Monitor for wandering visitors
- Watch for questions outside the visit's purpose
- Note visitors asking the same questions to multiple contractors
- Be alert to visitors becoming distraught when irregular questions aren't answered

Post-Visit Activities:

- Conduct debriefings with escorts, briefers, and hosts
- Document and report any anomalies or suspicious incidents
- Both programs are essential countermeasures that help protect classified and sensitive information while maintaining necessary international business relationships.

CI Trainings

The **32 CFR Part 117, NISPOM** requires contractors to provide all cleared employees with security trainings and briefings commensurate with their involvement with classified information to include initial and annual refresher trainings. Ongoing campaigns should be implemented to maintain vigilance against the threat posed by FIEs. This “vigilance campaign” should be tailored for situations common to your company employees, using a variety of communication methods, highlight key CI concepts, and reinforce reporting requirements and points of contact.

FSO RESPONSIBILITIES

- Provide initial and recurring training
- Ensure employees are aware of and follow reporting procedures
- Establish and implement company-specific standard operating procedures (SOPs) addressing responsibilities and requirements
- Utilize DCSA and CSA resources for defensive security and threat awareness training

AWARENESS STRATEGIES

- Monthly activities (poster contests, CI awareness, trivia, videos)
- CI awareness events with guest speakers from DCSA or other agencies
- Visual reminders throughout the facility (posters, flyers)
- Company website and social media messaging
- Resources from CDSE’s CI Toolkit

EFFECTIVE CI AWARENESS PROGRAM

- Goes beyond annual CI briefings to include an ongoing "vigilance campaign"
- Tailors content to situations common to company employees
- Uses varied communication methods
- Highlights key CI concepts
- Reinforces reporting requirements and points of contact

This comprehensive approach ensures continuous awareness and vigilance against threats posed by FIEs and other adversaries.

Threat Information Reporting

The NISPOM requires employees of cleared industry to report events that impact the status of the facility clearance (FCL), impact the status of an employee's personnel security clearance, affect proper safeguarding of classified information, or indicates that classified information was lost or compromised. Contractors are required to establish internal procedures to ensure that cleared employees are aware of their responsibilities for reporting pertinent information.

REPORTABLE INCIDENTS

- Mishandling of classified information
- Computer system misuse
- Suspicious cyber incidents
- Foreign influence
- Suspicious contacts
- Unauthorized use of recording devices
- Adverse information concerning cleared employees
- Actual, probable, or possible espionage, sabotage, terrorism, or subversive activities

REPORTING CHAIN

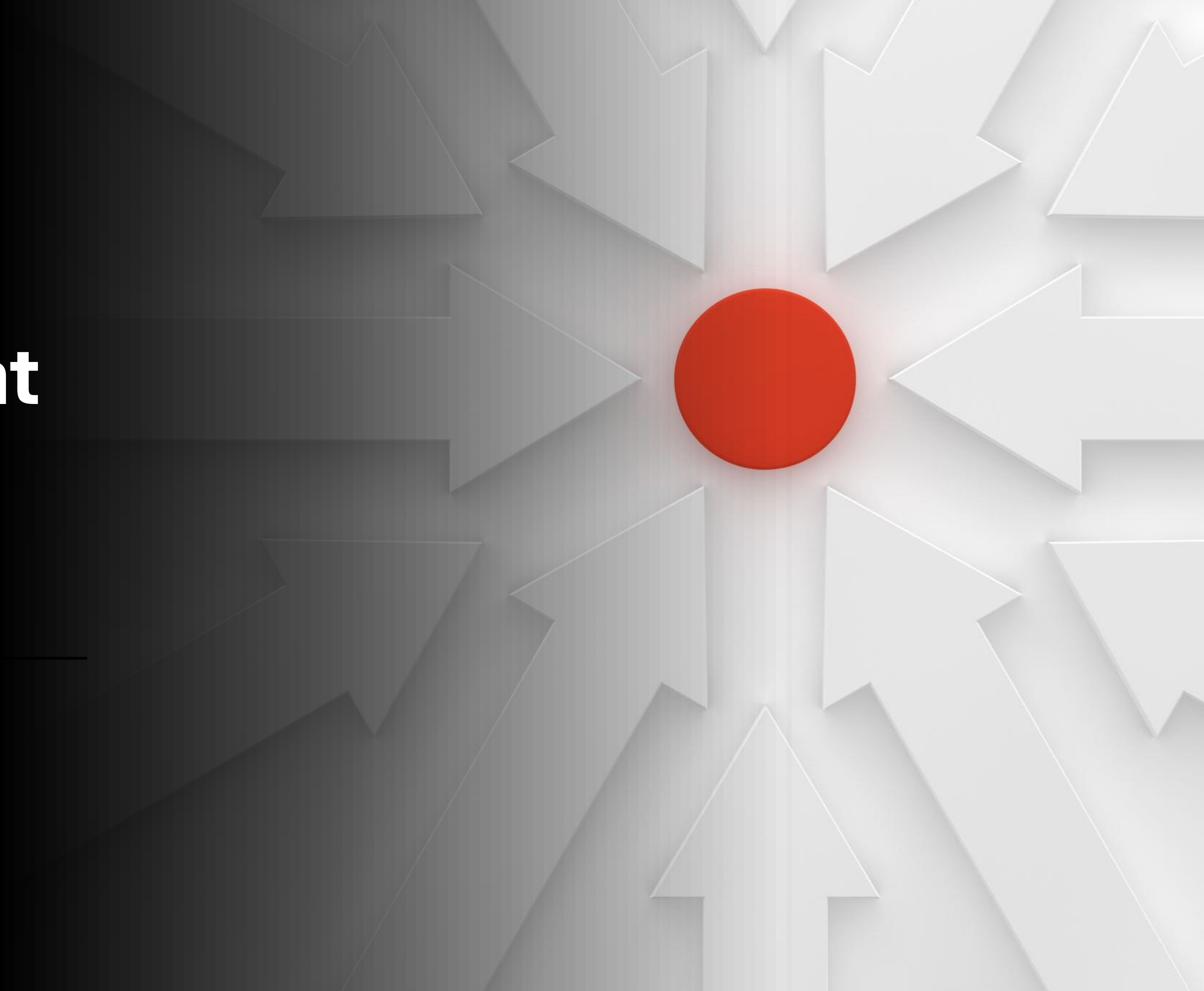
- **Employees report to:**
  - Facility Security Officer (FSO)
- **FSOs report to:**
  - DCSA (Cognizant Security Agency) via:
    - DCSA Industrial Security Representative (ISR), or
    - DCSA CI Special Agent (SA)

Espionage-related reports must be sent immediately to the FBI with a follow-up report to DCSA

- Initial FBI reports can be made by phone
- Must be followed by written reports

Reporting does not reflect negatively on your facility.
Reporting helps identify larger threats across cleared facilities and enables development of effective countermeasures.

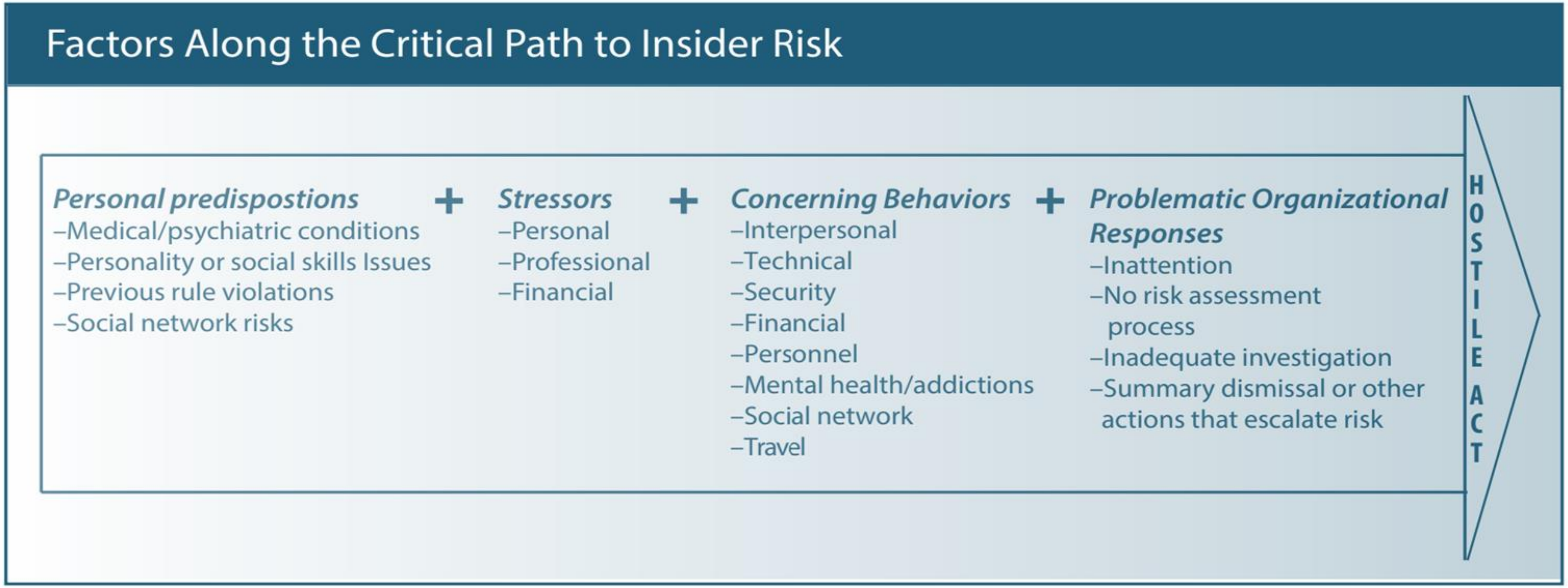
The best way to defeat the threat is to report the threat!



Insider Threat Mitigation Responses

The Critical Path: "The Proverbial Left of Boom"

Exemplary insider threat programs are designed to detect potential insider threat at the earliest stages possible, and to take action to prevent an insider event. The Critical Path Method outlines how to best detect potential insider threat.



Factors Along the Critical Path to Insider Risk

Personal predispostions **+**
- –Medical/psychiatric conditions
- –Personality or social skills Issues
- –Previous rule violations
- –Social network risks

Stressors **+**
- –Personal
- –Professional
- –Financial

Concerning Behaviors **+**
- –Interpersonal
- –Technical
- –Security
- –Financial
- –Personnel
- –Mental health/addictions
- –Social network
- –Travel

Problematic Organizational Responses
- –Inattention
- –No risk assessment process
- –Inadequate investigation
- –Summary dismissal or other actions that escalate risk

HOSTILE ACT

Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)

However, should you not be able to deter or detect, and an insider threat event happens, you must be able to respond quickly and effectively to limit damage to your organization and its mission.

The Response Framework and Mitigation

The response framework includes (check your own company Insider Threat plan for any unique procedures):

- **Policy, Process, and People.**
  - Your response plan should outline authorities and roles and responsibilities of stakeholders.
- **Initial Triage.**
  - Assess the threat to your organization/mission. Is the individual harming the organization's ability to execute its mission?
- **Stakeholder Coordination.**
  - Based on your threat assessment, insider threat programs should have clear policies concerning which stakeholders are engage and when. Develop thresholds for escalation up the management chain.
- **Investigate/Inquire.**
  - Conduct due diligence ensuring (1) protection of employee civil liberties and privacy and (2) administrative inquiry integrity (generally, the subject should not be notified). Document facts and patterns, being mindful that compromise of raw information could undermine the reputation of your program, and employee morale.
- **Containment.**
  - Depending on potential damage (network, reputation, infosec), work with stakeholders move to contain the damage quickly.
- **Remediate/After Action.**
  - Conduct after action assessments, including tabletop exercises, that seek to identify weaknesses in your response plan. Remediate any gaps with new policies and procedures.

Response Plans Are Multidisciplinary

- At the highest level of analysis, responses are organizational and individual.
  - **<u>Organizational</u>** responses might include enterprise level changes to security, human resource processes, or ethics and compliance standards.
  - **<u>Individual</u>** responses might include remedial or enhanced training, counseling, or graduated scale of discipline for insider threat subjects.
- Invariably, responses will involve personnel security, information security, counterintelligence, human resources, legal, business lines, and employee assistance programs.
- Develop scenarios of various types of insider threats (unintentional, negligent, malicious) from varying parts of your organization and plan for how you would respond – who would be involved, and how, if at all, you might escalate to organizational leadership or federal investigative entities.
- <u>Vigilance and Resilience – Corporate Culture</u>
  - Build corporate cultures that make employees feel safe in reporting potential indicators of insider threat. Anonymous reporting mechanisms should be available
  - Train employees on insider threat
  - As a best practice, ensure insider threat policies are updated at least annually

Reporting Requirements

There are at least four sets of controlling authorities on reporting insider threat events:

1. **DoD – Defense Insider Threat Management and Analysis Center (DITMAC)**
   - DoD Requirements for reporting to DITMAC can be found here: https://ditmac.experience.crmforce.mil/reporting/

2. **NISPOM – codified at 32 CFR, Part 117, SEAD 3.**
   - Pursuant to this rule, Security Executive Agent Directive (SEAD) 3, (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf*) and CSA-provided guidance to supplement unique CSA mission requirements, contractors and their cleared employees are required to:
     - *Report certain events that may have an effect on the status of the entity's or an employee's eligibility for access to classified information; report events that indicate an insider threat to classified information or to employees with access to classified information; report events that affect proper safeguarding of classified information; and report events that indicate classified information has been, or is suspected to be, lost or compromised.*

3. **FBI – Section 811 of the Intelligence Authorization Act of 1995**
   - Mandates the Federal Bureau of Investigation (FBI) is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to an agent of a foreign power.

4. **Military Departments – DoD Directive 5240.06, *Counterintelligence Awareness and Reporting*, Enclosure 4 - Reporting**
   - DoD personnel shall report potential FIE threats to their organization's CI element or their supporting MDCO.

Laws & Regulations, Record Checks

Records Check Overview

To evaluate potential insider threats and recommend mitigation actions you must gather comprehensive background information (record checks completed pre-employment, upon predication):

- Identify anomalous behaviors/attributes linked to insider threats
- Understand legal/privacy considerations in handling records
- Know what types of records to review

Key Considerations:

- Administrative Function: Not a formal investigation
- Respect Privacy (Privacy Act 1974, HIPPA, EO 12333)
- Preserve Viability: Avoid alerting individuals prematurely

Potential Records to Review:

- **Employment**: History, security records, performance
- **Military**: Promotions, punishments, foreign service
- **Medical**: Mental/physical health (with proper authority)
- **Law Enforcement**: Criminal, traffic, UCMJ violations
- **Civil/Financial**: Bankruptcy, liens, credit reports
- **Residential**: Verified addresses, associations
- **Education**: Degrees, activities, disciplinary records
- **Foreign Travel**: Destinations, contacts, purpose
- **Citizenship**: Status, documentation, foreign ties

Locating Information

Insider Threat Programs access various lawful data sources based on agency type (DOD, Federal, or Industry). You should be able to access your organization's records and any open sources/publicly available data. DOD, Federal, or Industry Programs should consult respective Insider Threat Program's Standard Operating Procedures (SOP). Your organization may have Memoranda of Agreement, policies, or other procedures in place to facilitate lawful access to additional sources.

Key Data Source Categories

- **DOD Sources**
  - PSI File, DMDC, DCII, DISS, DSOS, DITMAC
  - Only available to DOD Components
- **Federal Sources**
  - HR Files, SEVIS, FinCEN, NCIC, TECS, Consolidated Screening List
  - Contact agencies directly (with Privacy Act advisement)
- **Open & External Sources (see individual Corporate Legal Department)**
  - Internet - blogs, social media — Publicly Available Electronic Information (PAEI) rules apply.
  - Employment, residential, birth, and education records
  - Foreign travel (State Department passports, Customs/Border Patrol, agencies – TSA, etc.)

Verifying and Corroborating Information

Information verification is essential for ensuring credibility and preventing misinformation. Primary sources provide original, firsthand accounts while secondary sources analyze or interpret primary sources. Verify information by assessing source credibility and cross referencing with other reputable sources.

Why Use Multiple Data Sources?

- Conflicting information is common—verification is essential.
- Use multiple sources to:
    - Corroborate data
    - Identify discrepancies
    - Uncover exculpatory (clearing) evidence
- Incomplete or incorrect info must be further investigated.

Impact of Inaccurate Information

Allegations can seriously affect an individual's career. Decisions must be based on verified, complete, and balanced facts.

Aim for an accurate assessment before determining any response.

- **Primary vs. Secondary Sources**
- Primary Source: Direct evidence (e.g., court documents, credit reports).
- Secondary Source: Secondhand information (e.g., interviews).
- Best Practice: Use primary sources whenever possible.
    - If using secondary sources, corroborate with multiple sources

Risk Indicators from Databases/Electronic Records

Potential risk indicators (PRIs) in records, databases, and other forms of information.

Effective Risk Indicators:

- Observable – information from reliable source IAW laws and regulations
- Valid – relevant
- Reliable – consistent data collection methods and indicator definitions.
- Stable – monitoring over time, track indicators and any changes
- Unique – indicators measure one thing, and can be aggregated with others to indicate risk

DOD Potential Risk Indicators (DITMAC)

- Access attributes
- Professional lifecycle and performance
- Foreign Considerations
- Security Compliance and Incidents
- Technical Activity
- Criminal, violent, or abusive conduct
- Financial Considerations
- Substance abuse and addictive behaviors
- Judgement, character, and psychological conditions

DOD Component Insider Threat Programs may reference DITMAC for the most current PRIs and detailed explanations of each category. All Insider Threat Programs are encouraged to coordinate with their cognizant authorities to maintain current indicators.

Information Shared Internally & Externally

Internal Sharing

- Share relevant indicators with your Insider Threat Program per your SOP. (ex. HR, Legal, IT/CISO, Ethics)
- Purpose: Support risk assessment and identify mitigation options.

External Reporting – varying thresholds

- **FBI Notification** (Section 811, Intelligence Authorization Act):
  - Immediate referral required for possible/probable compromise of classified info.
  - Activity pauses until FBI guidance is received.
- **Additional Notifications:**
  - **DOD Programs:** Notify Military Department Counterintelligence Office (per DODI 5240.10).
  - **Industry Programs:** Notify DCSA (per NISPOM, 32 CFR Part 117.8).

Other Required Reports (DOD):

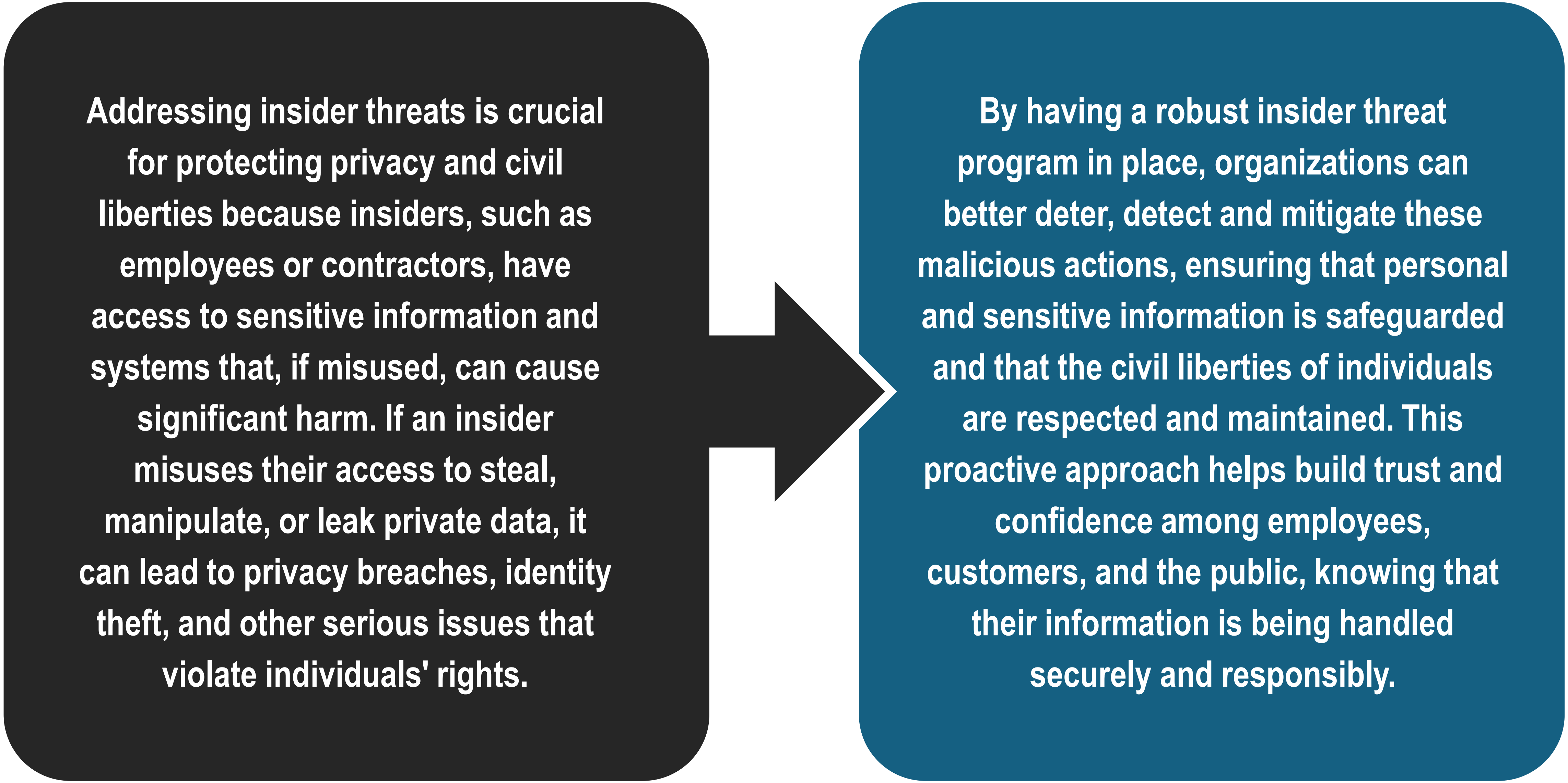
- Imminent threats to people or property
- Criminal activity
- Compromise of resources
- Any threshold established by DITMAC

Legal Considerations

- Protect privacy (PII, HIPAA)
- Secure transmissions
- Follow classification guidelines
- Consult General Counsel as needed

Protecting Privacy & Civil Liberties in Insider Threat Programs

Impact on Privacy and Civil Liberties



Addressing insider threats is crucial for protecting privacy and civil liberties because insiders, such as employees or contractors, have access to sensitive information and systems that, if misused, can cause significant harm. If an insider misuses their access to steal, manipulate, or leak private data, it can lead to privacy breaches, identity theft, and other serious issues that violate individuals' rights.

By having a robust insider threat program in place, organizations can better deter, detect and mitigate these malicious actions, ensuring that personal and sensitive information is safeguarded and that the civil liberties of individuals are respected and maintained. This proactive approach helps build trust and confidence among employees, customers, and the public, knowing that their information is being handled securely and responsibly.

Legal Protections

- **1st Amendment:** Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

- **4th Amendment:** The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

- **5th Amendment:** No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

- **9th Amendment:** The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

- **14th Amendment**, Section 1: All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law that shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Legal and Regulatory Framework

Key laws and regulations protecting privacy and civil liberties:

The General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA) are key laws designed to protect privacy and civil liberties. GDPR, enacted by the European Union, sets a high standard for data protection and privacy for individuals within the EU, requiring organizations to obtain explicit consent for data collection, maintain data accuracy, and ensure secure processing. HIPAA, a U.S. law, protects sensitive patient health information from being disclosed without the patient's consent or knowledge, mandating standards for electronic health care transactions and requiring safeguards to protect health data privacy.

Organizational policies that support these regulations:

The CCPA, a landmark state law in California, grants residents the right to know what personal data is being collected about them, to whom it is being sold, and the right to access, delete, and opt-out of the sale of their personal data. Together, these laws create frameworks for protecting individual privacy and granting people greater control over their personal information.

Privacy Act

The Privacy Act of 1974 is a crucial U.S. federal law enacted to protect personal information held by federal agencies. It establishes a framework for the collection, maintenance, and dissemination of personal data, ensuring transparency, consent, and security. The Act grants individuals the right to access and amend their records, promoting data accuracy and integrity. It requires agencies to inform individuals about data practices, obtain consent before sharing information, and implement safeguards to protect data against unauthorized access.

The Act also places responsibilities on federal agencies to limit data collection to necessary information and ensure the security of personal data. While there are specific exemptions for national security and law enforcement, these must be documented and published. The Office of Management and Budget (OMB) oversees compliance, with agencies required to submit annual reports to Congress. Overall, the Privacy Act of 1974 enhances public trust by ensuring that personal information is handled responsibly by federal agencies.

Personally Identifiable Information (PII)/Protected Health Information (PHI)

PII refers to any information that can be used to identify a specific individual. This includes details like your name, address, phone number, email address, Social Security number, or any other information that can be linked to you personally. Essentially, if a piece of information can be used to figure out who you are, it's considered PII.

PHI is a specific type of personal information related to your health. It includes any medical records or other details about your health status, treatments, or healthcare services. PHI can include things like your medical history, test results, insurance information, and doctor’s notes. This information is protected under laws like the Health Insurance Portability and Accountability Act (HIPAA) to ensure your privacy in healthcare settings.

Reasonable Expectation of Privacy

The "Reasonable Expectation of Privacy" in the context of an organization's computer network refers to the understanding and policies regarding employees' privacy when using company-owned devices and networks.

Key points include:

1. Clear Policies:

- The organization should have clear, written policies outlining what level of privacy employees can expect when using the company's computer network and devices. This includes email, internet use, and any data stored on company systems.

2. Employee Awareness:

- Employees should be informed and acknowledge that their activities on the organization's network may be monitored and are not entirely private. This information is usually provided through onboarding, regular training, and signed agreements.

3. Monitoring and Security:

- Organizations typically monitor network usage to ensure security, prevent data breaches, and maintain operational integrity. Employees should understand that this monitoring is in place to protect both the organization and its stakeholders.

4. Balanced Approach:

- While monitoring is necessary, organizations should balance it with respect for employees' privacy, ensuring that surveillance is reasonable, transparent, and not overly intrusive.

By setting clear expectations and communicating them effectively, organizations can manage privacy concerns while maintaining necessary security and operational standards on their computer networks.

Freedom of Information Act (FOIA)

	The Freedom of Information Act (FOIA) is a U.S. law that gives the public the right to access information from the federal government. It ensures transparency and accountability by allowing citizens to request and obtain federal agency records, with certain exceptions. Key points about FOIA:
Public Access:	FOIA allows anyone to request access to federal government records, regardless of their purpose for the request.
Request Process:	Requests must be made in writing and reasonably describe the information sought. Federal agencies are required to respond to FOIA requests within a certain timeframe.
Exemptions:	Some information is exempt from disclosure under FOIA. Exemptions include national security, personal privacy, trade secrets, and law enforcement records.
Appeals and Judicial Review:	If a request is denied, requesters can appeal the decision within the agency or take the matter to court for judicial review.
Enhancing Transparency:	FOIA helps ensure government transparency by making it easier for the public to access government documents and understand government activities.
	Overall, FOIA is a powerful tool for promoting openness and accountability in the federal government.

Balancing Security and Privacy

Ensuring security measures do not infringe on privacy rights:

- Balancing security and privacy is essential to ensure that protective measures do not infringe on individuals' rights. One key approach is to minimize data collection and limit access strictly to what is necessary for operational purposes, thereby reducing the potential for misuse or unauthorized exposure. Where feasible, organizations should anonymize data to protect identities, ensuring that personal information cannot be linked back to specific individuals. Transparency is critical; clear policies regarding data usage and monitoring should be communicated to all stakeholders, so everyone understands what data is collected, why it is collected, and how it is used.

Role of privacy officers and compliance teams

- Privacy officers and compliance teams play a vital role in this balance, overseeing the implementation of privacy safeguards, ensuring adherence to relevant laws and regulations, and serving as points of contact for addressing any privacy concerns. By adopting these measures, organizations can protect their systems and data while respecting and upholding the privacy rights of individuals.

Consequences of misuse of information

- Serious civil, criminal and administrative penalties may apply

Course Conclusion

Insider threats are real and continue to evolve – even individuals who are well-meaning can, unintentionally, cause harm to an organization

Early detection of indicators of insider threat is essential to protect an organization’s classified and sensitive programs, personnel, information, and reputation

Incorporating counterintelligence or CI and threat awareness into your program makes your program stronger and more successful

Insider Threat Programs mitigate the threats posed by witting and unwitting insiders through the deployment of multidisciplinary responses

Insider Threat Programs utilize records checks to support the identification of anomalous behavior associated with insider threats

Insider Threat Programs have the responsibility to ensure its actions do not infringe on any individual’s legal privacy and civil liberties

Course Conclusion

This concludes the training for Insider Threat Program Personnel.

Please print your name and include the date of completion on the certificate in the next slide.

Certificate of Completion

This certifies that

[INSERT NAME HERE]

has successfully completed the training requirements set forth in

NISPOM 117.12(g)(1) for Insider Threat Program Personnel

Date of Completion: ____________________

References

- 32 CFR 117.12(g)(2) - eCFR :: 32 CFR Part 117 -- National Industrial Security Program Operating Manual (NISPOM)
- Targeting US Technologies - DCSA-TA-25-001 Unclassified Targeting U.S. Technologies A Report of Threats to Cleared Industry FY24.pdf
- DITMAC Reporting - https://ditmac.experience.crmforce.mil/reporting/
- SEAD-3 - *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf*
- FBI – Section 811 of the Intelligence Authorization Act of 1995 - H.R.4299 - 103rd Congress (1993-1994): Intelligence Authorization Act for Fiscal Year 1995 | Congress.gov | Library of Congress
- DoD Directive 5240.06, *Counterintelligence Awareness and Reporting*, Enclosure 4 – Reporting - DoDD 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, Incorporating Change 3 on August 31, 2020
- Privacy Act 1974 - Office of Privacy and Civil Liberties | Privacy Act of 1974
- HIPPA - Privacy | HHS.gov
- EO 12333 - Executive Orders | National Archives
- DODI 5240.10 - DoD Issuances
- CCPA (California Consumer Privacy Act) - California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General
- General Data Protection Regulation - General Data Protection Regulation (GDPR) – Legal Text
- NISP Tools and Resources - NISP Tools & Resources
- DCSA CDSE Insider Threat Toolkit - Insider Threat Toolkit