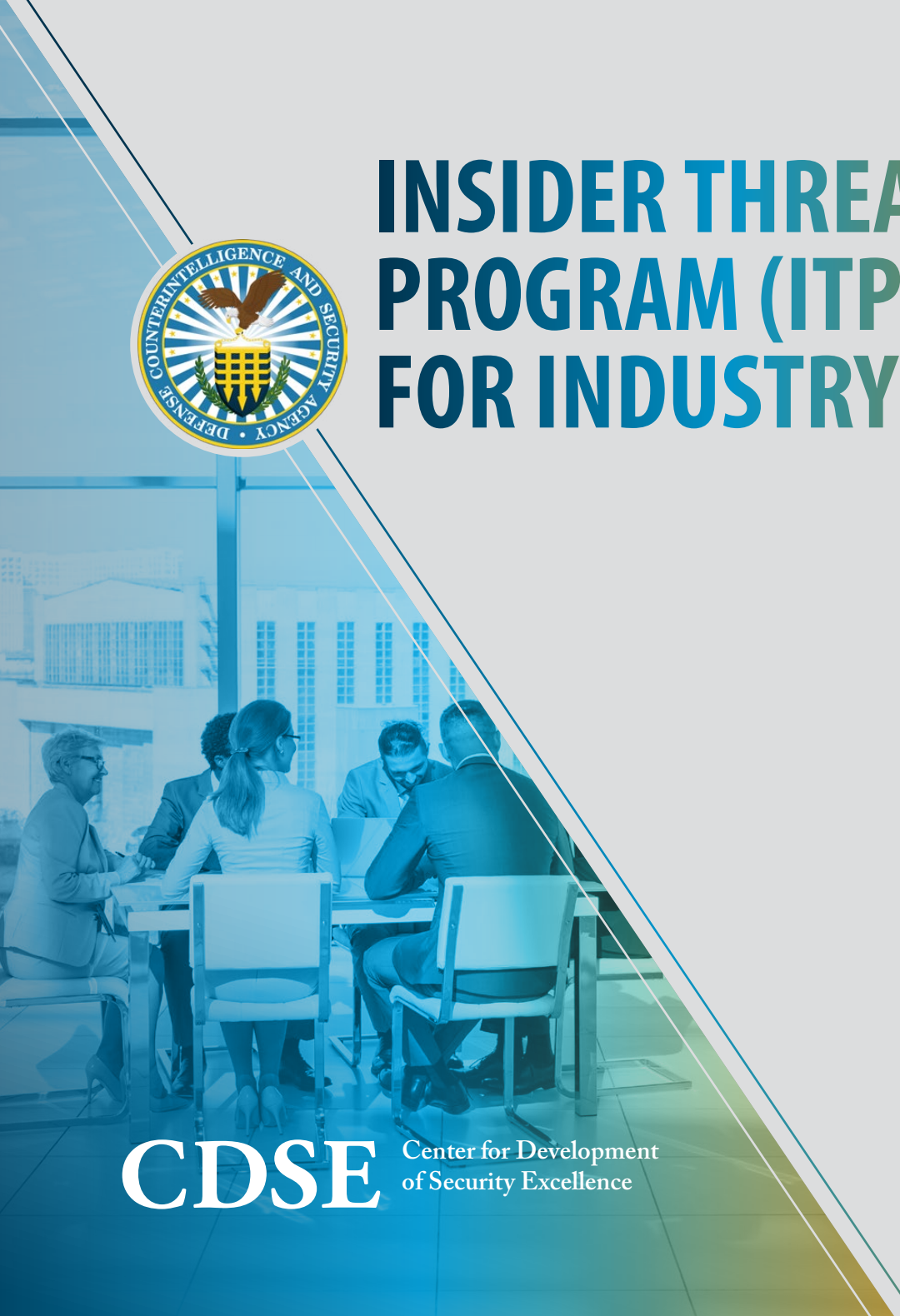
MAY 2022

INSIDER THREAT PROGRAM (ITP) FOR INDUSTRY

JOB AID



CDSE Center for Development of Security Excellence

INTRODUCTION

This job aid gives Department of Defense (DOD) staff and contractors an overview of the insider threat program requirements for Industry as outlined in the National Industrial Security Program Operating Manual (NISPOM) that became effective as a federal rule in accordance with 32 Code of Federal Regulations Part 117, also known as the "NISPOM Rule." This job aid addresses policy, responsibilities, requirements, and the procedures consistent with Executive Orders (EO), 12869, "National Industrial Security Program;" EO 10865, "Safeguarding Classified Information and Security;" and 32 CFR Part 2004, "National Security Industrial Security Program."

CONTENTS

Click the individual links to view each topic.

ESTABLISH AN INSIDER THREAT PROGRAM

On October 7, 2011, the President signed **Executive Order 13587**, "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." Executive Order (EO) 13587 directs the heads of agencies that operate or access classified computer networks to have responsibility for appropriately sharing and safeguarding classified information.

In November 2012, the White House issued **National Insider Threat Policy for Executive Branch Agencies**. These minimum standards provide the departments and agencies with the minimum elements necessary to establish effective Insider Threat Programs and safeguard classified information.

On February 24, 2021, **32 CFR Part 117**, "National Industrial Security Program Operating Manual (NISPOM)" became effective as a federal rule. Referred to as the "NISPOM rule," it provides the contractor no more than six months from this effective date to comply with the requirements stipulated therein. Per 117.7(d), these requirements are consistent with the aforementioned E.O. 13587 and National Insider Threat Minimum Standards.

REQUIREMENTS

32 CFR Part 117 has identified the following requirements to establish an Insider Threat Program:

- Designate an Insider Threat Program Senior Official (ITPSO) who is cleared in connection with the facility clearance. If the appointed ITPOS is not also the Facility Security Officer (FSO), the ITPSO will ensure the FSO is an integral part of the contractor's insider threat program.
- The ITPSO will establish and execute an insider threat program and self-certify the Implementation Plan in writing to DSCA.
- Establish an Insider Threat Program group (program personnel) from offices across the contractor's facility, based on the organization's size and operations.
- Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.
- Monitor classified network activity.
- Gather, integrate, and report relevant and available information indicative of a potential or actual insider threat to deter employees from becoming insider threats; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.
- Conduct self-inspections of Insider Threat Programs.

GETTING STARTED

Establishing your Insider Threat Program involves more than checking off the requirements. The program requires an implementation plan to gather, share, integrate, identify, and report relevant Insider Threat information from offices across the contractor's facility including security, information security, and human resources; this is based on the organization's size and operations. The Senior

Management Program Official will need to outline the program and identify staff responsible for planning, implementing, and operating each element. It may be helpful to break the process down into phases.

During the **Evaluation Phase**, you will need to consider whether existing company policies and procedures are in line with the NISPOM Rule if changes, updates, or additional items are required. During the **Formulation Phase**, you can develop a plan or add to an existing plan for implementing each requirement under your Insider Threat Program. This job aid will assist you with each requirement area. Click each link on the **main page** for an overview of the requirement, advice for getting started, best practices, and related policy and training resources. During the **Implementation Phase**, your Insider Threat Program will be formally launched and operational.

Note that during the 6-month implementation period, the SMO must self-certify that they have an implementation plan for insider threat. The self-certification must be in writing (i.e., letter, email). The company is not required to submit the full plan during the implementation phase, but simply a certify that the company has a plan in place.

This self-certification must come from the SMO at the company or facility and must be via email, letter, or other written form. NOTE: if one plan is certified for the company, each local facility must provide the certification to their assigned ISR. Full written plans must be made available to DCSA upon request and will be part of the review during the SVA.

BEST PRACTICES

While the requirements identified in the NISPOM Rule make up the baseline for establishing an Insider Threat Program, you may find it helpful to further break out associated duties and responsibilities. Consider the list of core elements when planning your program. Also, remember that organizations both large and small have the same minimum requirements, but larger companies will likely have more complex processes for implementation.

Insider Threat Programs are designed to mitigate risk and thus fit into your facility's overall risk management practices.

RELATED TRAINING AND RESOURCES

- eLearning Course: **Establishing an Insider Threat Program for Your Organization INT122.16**
- Insider Threat Toolkit Tab: **Establishing a Program**

DESIGNATE AN INSIDER THREAT SENIOR OFFICIAL

REQUIREMENTS

32 CFR Part 117 or the NISPOM Rule (Section 117.7(b) (2) clarifies the responsibilities of the Senior Management Official (SMO) i117.7(b) (2) of each cleared entity to better reflect the critical role and accountability of this position for entity compliance with the NISPOM Rule. The change further emphasizes the essential role of the SMO with the entity's security staff to ensure compliance.

- U.S. Citizen
- Employee
- Cleared in Connection with the Facility Clearance
- The Insider Threat Senior Official must always be cleared to the level of the facility clearance (FCL)

GETTING STARTED

The Insider Threat Program Senior Official may be the FSO or any other employee that meets the requirements. If the FSO is not chosen as the Insider Threat Senior Official, the FSO must still be an integral member of the facility's Insider Threat Program. A corporate family may choose to implement a corporate-wide Insider Threat Program with one senior official designated to establish and execute the program. Each cleared legal entity using the corporate-wide Insider Threat Program Senior Official must separately designate that person as the Insider Threat Senior Official for that legal entity and include them on the Key Management Personnel (KMP) list. When a division or branch has been granted an FCL based on requirement for safeguarding, the division or branch may designate the corporate-wide Insider Threat Program Senior Official as a KMP or designate a different employee to be the Insider Threat Program Senior Official at the division or branch.

The selected official must receive training on key topics related to Insider Threat and be able to demonstrate the effectiveness of their Insider Threat program to the CSA. The Senior Management Official will be responsible for implementation of the plans, processes, procedures and response protocols under the Insider Threat Program at the facility.

BEST 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.

RELATED TRAINING AND RESOURCES

- eLearning Course: **Establishing an Insider Threat Program for Your Organization INT122.16**
- Insider Threat Toolkit Tab: **Establishing a Program**

REPORT INSIDER THREAT INFORMATION TO THE CSA

32 CFR Part 117 addresses the reporting requirements in section 117.8. Additionally, 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, and Industrial Security Letters (ISL) that can be accessed via the **DCSA Industry Tools Tab (Industry Security Letters**).

REPORTING REQUIREMENTS

- 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
- Report events that indicate classified information has been, or is suspected to be, lost or compromised.
- Report promptly in writing to the nearest field office of the Federal Bureau of Investigation regarding information coming to the contractor's attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations.

GETTING STARTED

As part of your facility's overall risk mitigation strategy, the Insider Threat Program is designed to identify indicators, behaviors, and activities associated with potential insider threats and report them appropriately. Events that impact the following MUST be reported to the Facility Security Officer (FSO), DCSA, and in some instances the FBI:

- The status of the facility clearance
- The status of an employee's personnel security clearance
- That indicate an employee poses a potential Insider Threat
- That affect proper safeguarding of classified information
- That indicate classified information has been lost or compromised

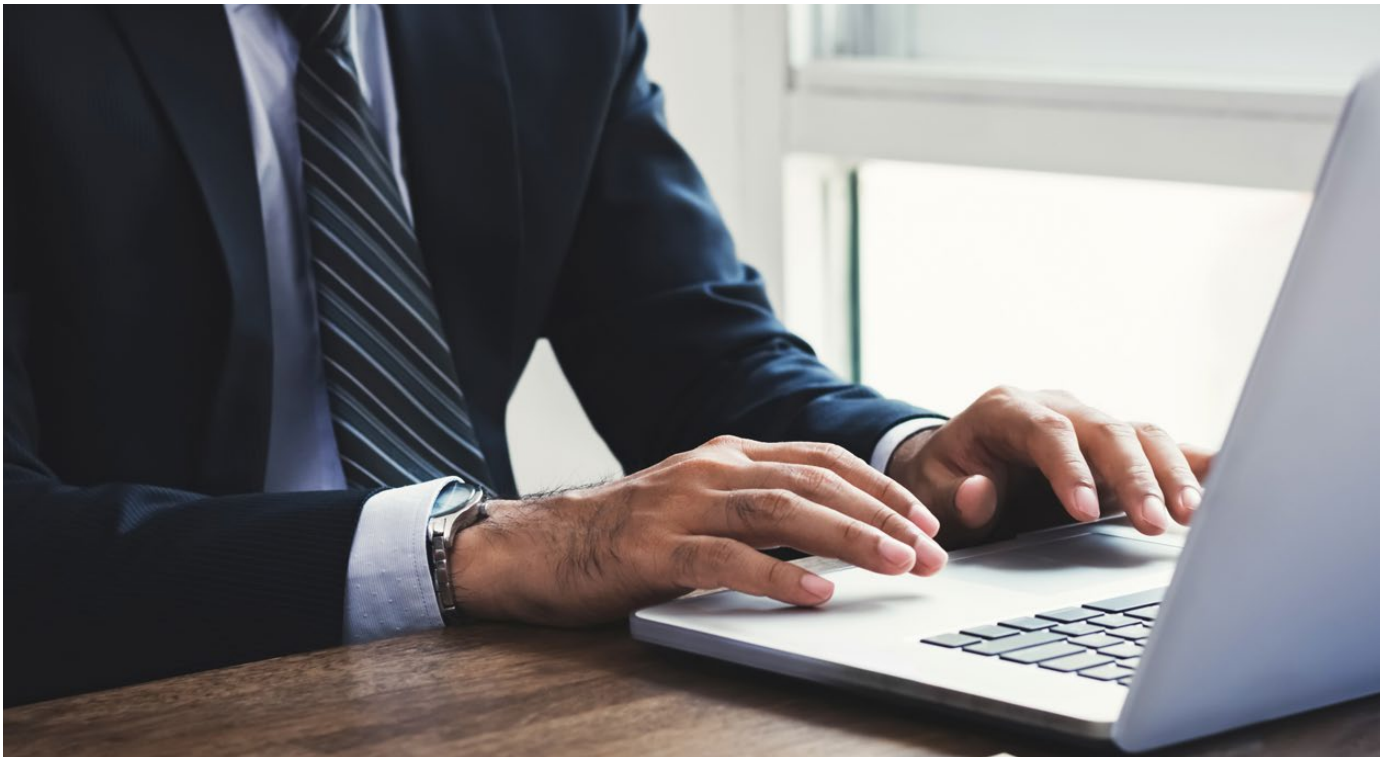
Once reported through appropriate channels steps will be taken by responsible parties to analyze the data and take further action. Information reported to DCSA may be referred to cognizant security, law enforcement, and intelligence agencies including Military Department law enforcement, intelligence, and counterintelligence activities; Defense Insider Threat Management Analysis Center (DITMAC); Central Adjudication Facilities (CAFs); and/or local, state, and federal law enforcement as appropriate. Your Insider Threat Program is responsible for identifying and reporting indicators – not prosecuting individuals. It should be noted that mitigating factors often exonerate individuals identified through the program and/or identify security vulnerabilities and appropriate countermeasures.

BEST PRACTICES

- Reporting refers to the transfer of information to the CSA and appropriate authorities. However, it also refers to actions taken by employees to inform the Insider Threat Program of actual or suspected insider threat activities and indicators.
- Ensure that the Insider Threat Program group (program personnel from offices across the contractor's facility based on the organization's size and operations) encourages reporting from personnel and information under their area of responsibility.
- All employees are required to take Insider Threat Awareness training which identifies reportable behaviors and activities. Consider supplementing this annual training with newsletters, job aids, posters and other material to reinforce reporting requirements and responsibilities.
- Work with your DCSA Counterintelligence Special Agent, Industrial Security Representative, and Information System Security Professional to identify appropriate response actions including reporting and the development of countermeasures.

RELATED TRAINING AND RESOURCES

- eLearning Course: **Adverse Information Reporting**
- eLearning Course: **The 13 Adjudicative Guidelines**
- eLearning Course: **Insider Threat Awareness**
- Insider Threat Toolkit Tab: **Reporting**
- **Insider Threat Job Aids/Case Studies**



CONDUCT INSIDER THREAT TRAINING

32 CFR Part 117 requires that the designated Insider Threat Program Senior Official ensure that contractor program personnel assigned insider threat program responsibilities and all other cleared employees complete training consistent with applicable CSA guidance.

INSIDER THREAT TRAINING REQUIREMENTS

Section 117.12 of 32 CFR Part 117 has identified the following requirements for the conduct of insider threat training:

- Contractor Insider Threat Program personnel, including the contractor designated Insider Threat Program Senior Official, must be trained in:
  - (1) Counterintelligence and security fundamentals, including applicable legal issues.
  - (2) Procedures for conducting Insider Threat response actions.
  - (3) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.
  - (4) Applicable legal, civil liberties, and privacy policies.
- All cleared employees must be provided Insider Threat awareness training annually and before being granted access to classified information, and annually thereafter. Training will address current and potential threats in the work and personal environment and will include the following information at a minimum:
  - (1) The importance of detecting potential Insider Threats by cleared employees and reporting suspected activity to the Insider Threat Program designee.
  - (2) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems.
  - (3) Indicators of Insider Threat behavior, and procedures to report such behavior.
  - (4) Counterintelligence and security reporting requirements, as applicable.

The contractor will establish procedures to validate all cleared employees who have completed the initial and annual insider threat training.

GETTING STARTED

Getting started on your Insider Threat Training is as easy as heading over to the DCSA Training Directorate, the Center for Development of Security Excellence (CDSE) **website**. CDSE provides numerous courses on counterintelligence awareness, security fundamentals, and Insider Threat. The "**Insider Threat Awareness**" course has been approved by the National Insider Threat Task Force (NITTF) as meeting the minimum standards for initial and annual Insider Threat Awareness Training. "**Establishing an Insider Threat Program**" covers essential procedures for setting up shop and addresses many of the requirements for training Insider Threat Program personnel. Consult your legal counsel to enhance training in the areas of gathering, retaining and safeguarding information AND

legal, civil liberties, and privacy policies. Your company likely has policies and accompanying training on these issues already in place. Access the CDSE's **Insider Threat Toolkit** for more information on Awareness & Training, Policy/Legal, Reporting, Establishing a Program, and Cyber Insider Threat.

Note: Insider Threat Program Senior Official (ITPSO) training must be completed within the 6-month implementation phase. If a new official is appointed after the 6-month implementation period, they must complete the required training within 30-days of being assigned ITSO responsibilities. ITPSOs may take CDSE course "Establishing an Insider Threat Program for your Organization" (course INT122.16) in STEPP to receive credit or may develop independent training for the ITPSO.

Employee training on insider threat must be taken prior to an employee being granted access to classified information or within 12 months of policy implementation. This training may be part of their initial security briefing and annual refresher training so long as the required topics as outlined in the NISPOM Rule are covered in their entirety. Records shall be maintained for initial and refresher insider threat training.

GETTING STARTED

- Designate an Insider Threat Program Group team member, who can also be the FSO, with responsibility for education, training, and awareness. It's a good idea for someone in the program to regularly attend refresher training on new security awareness training topics.
- Remember, while initial and annual refresher training may be the requirement, effective training is not merely an event, but a process. Continue to seek out new sources of information to reinforce learning and awareness of the Insider Threat. **CDSE** provides free security posters, job aids, and brochures that are regularly updated.
- Consider Insider Threat awareness training for contractors, vendors, and trusted business partners. An "Insider" is defined as any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks or systems.

RELATED TRAINING AND RESOURCES

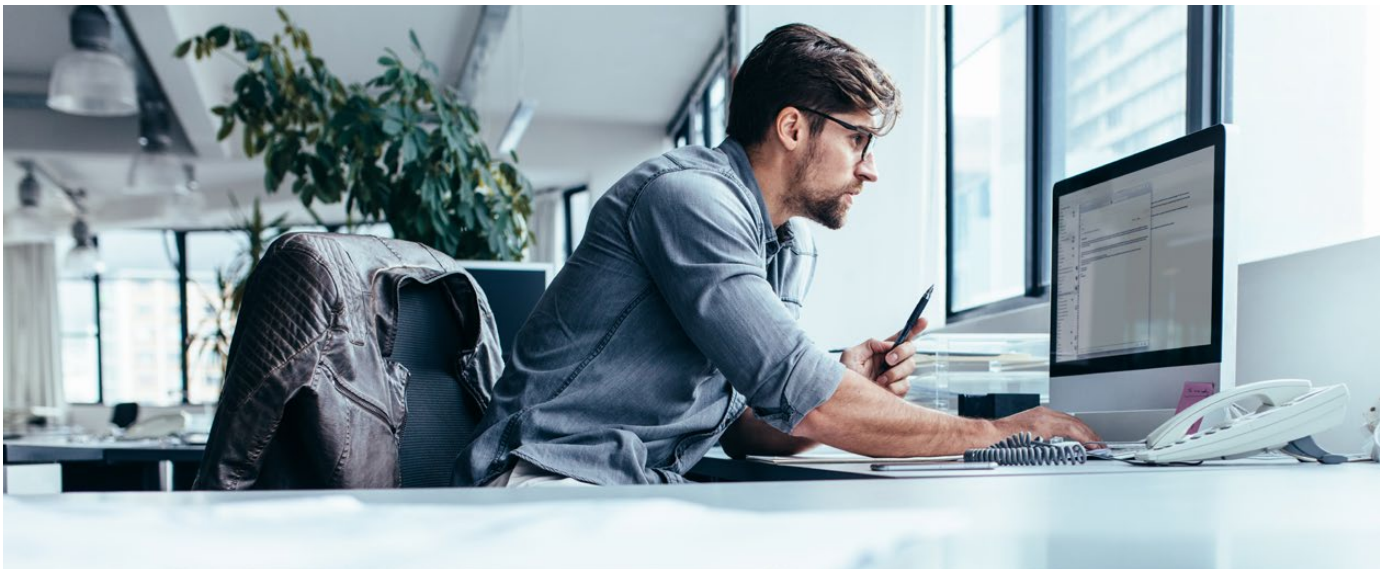
- eLearning Course for cleared personnel: **Insider Threat Awareness INT101.16**
- eLearning Course for Insider Threat Program Personnel: **Establishing an Insider Threat Program for Your Organization INT122.16**
- **Insider Threat Training**
- **Counterintelligence and General Security Resources**
- Insider Threat Toolkit Tab: **Awareness & Training**
- **CDSE Job Aids and Resources**

MONITOR CLASSIFIED NETWORK ACTIVITY

The Contractor will maintain an information system security program that supports overall information security by incorporating risk-based set of management, operational, and technical security controls in accordance with CSA-provided guidance. The contractor will incorporate into the program the following:

REQUIREMENTS

- User activity monitoring network activity, either automated or manual
- Information sharing procedures
- A continuous monitoring program
- Policies and procedures that reduce information security risks to an acceptable level and address information security throughout the information system life cycle
- Plans and procedures to assess, report, isolate, and contain data spills and compromises, to include sanitization and recovery methods
- Protecting, interpreting, storing and limiting access to user activity monitoring automated logs to privileged users
- Processes to continually evaluate threats and vulnerabilities to contractor activities, facilities, and information systems to ascertain the need for additional safeguards
- Change control processes to accommodate configuration management and to identify security relevant changes that may require re-authorization of the information system
- Methods to ensure users are aware of rights and responsibilities through the use of banners and user agreements
- Manager (ISSM) will ensure the functions of the Information System Security Officer (ISSO) and the system manager will not be performed by the same person



GETTING STARTED

- Governance, or the policies and procedures you enact for your Insider Threat Program, will guide your efforts in monitoring user activity on your organization's classified networks. These should include user and group management, use of privileged and special rights, and security and policy changes. Key components of governance include having employees sign agreements acknowledging monitoring and implementing banners informing users that their system and network activity is being monitored. Monitoring these components ensures that users' access is limited to what is essential for their role. This allows you to then prioritize monitoring efforts. It also allows you to identify users who are abusing their privileges.
- System Activity Monitoring will allow your program to identify possible system misuse. Activities or events to monitor include logons and logoffs, system restarts and shutdowns, and root level access. Monitoring these activities identifies when the network is being accessed, any potential software installs, and whether someone is accessing or making changes to the root directory of a system or network.
- User Activity Monitoring helps identify users who are abusing their access and may be potential Insider Threats. This includes monitoring file activities, such as downloads, print activities (such as files printed), and search activities. Monitoring these activities can identify abnormal user behaviors that may indicate a potential Insider Threat. While you cannot monitor every aspect of these activities, you can prioritize efforts as they relate to the systems and information that require the most protection.
- Key elements to your program will include monitoring considerations, integration, audit requirements, analysis and reporting.

BEST PRACTICES

- The ISSM plays an important role in the contractor's Insider Threat Program and reports information system activities related to the program to the contractor's Insider Threat Program Senior Official (ITPSO).
- Monitoring activity on classified networks is essential to the success of your Insider Threat Program.
- Successful monitoring will involve several levels of activities.
- Once policies are in place, system activities, including network and computer system access, must also be considered and monitored.
- Consider enforcing the principle of least privilege to facilitate limitations on access and the monitor and review of inconsistent access or privilege elevation.
- Finally, an Insider Threat Program must also monitor user interactions on the classified networks and information systems.

RELATED TRAINING AND RESOURCES

- eLearning Course: **Continuous Monitoring Course**
- Insider Threat Toolkit Tab: **Cyber Insider Threat**

CONDUCT SELF-INSPECTIONS OF THE INSIDER THREAT PROGRAM

32 CFR Part 117 addresses requirements for contractors conducting formal self-inspections, which includes the Insider Threat Program.

REQUIREMENTS

- Section 177.7 (C) (2) Contractor Reviews. Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.
- Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspection will include the review of samples representing the contractor's derivative classification actions, as applicable.
- The contractor will prepare a formal report describing the self-inspection, its findings, and resolution of issues discovered during the self-inspection. The contractor will retain the formal report for CSA review until after the next CSA security review is completed.
- A senior management official at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.

GETTING STARTED

Your facility is already conducting self-inspections and reviewing security systems in accordance with risk management principles. The new requirements indicate that you will add your Insider Threat Program to the self-inspection program for review. CDSE offers an eLearning course in **NISP Self-Inspection** practices and requirements. In addition, you can follow the guidance in the **NISP Self-Inspection Handbook**. Remember, your Industrial Security Representative is also a great resource and can guide you through the process.

BEST PRACTICES

Self-inspection provides an opportunity for audit and improvement, not only for the security program, but also for your Insider Threat Program. Consider these best practices:

- Identify accountabilities.
- Identify staff able to manage the overall process of an integrated self-inspection program.
- Identify self-inspection compliance to requirements.

- Evaluate appropriateness of performance indicators and metrics (metrics drive behavior).
- Plan and select a self-inspection approach.
- The self-inspection objectives should be clearly defined and understood by all involved.
- Validate the effectiveness of Insider Threat Awareness training.
- Evaluate reporting procedures and employee familiarity with requirements.
- Periodically evaluate new solutions to address Insider Threats.
- Remember that "one size does not fit all" and Insider Threat solution vendors may not support the same protocols and standards.
- Consider the usage of technical and behavioral potential Insider Threat risk indictors.
- Identify risks in your program.
- Identify and prioritize required improvements.

RELATED TRAINING AND RESOURCES

- eLearning Course: **NISP Self Inspection**
- **Self-Inspection Handbook for NISP Contractors**
- FSO Toolkit Tab: **Self-Inspections/Assessments**

DEFINITIONS AND REFERENCES

DEFINITIONS

Insider. Any person with authorized access to any government or contractor resource to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat. The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of National Security Information (NSI) or through the loss or degradation of government, company, contract or program information, resources, or capabilities.

Insider Threat Program. A coordinated group of capabilities under centralized management that is organized to detect and prevent the unauthorized disclosure of sensitive or classified information. At a minimum, an Insider Threat program shall consist of capabilities that provide access to information; centralized information integration, gathering and analysis of information, and reporting to the appropriate agency; employee Insider Threat awareness training; and the monitoring of user activity on government computers.

REQUIREMENTS

- Designate an Insider Threat Program Senior Official (ITPSO) who is cleared in connection with the facility clearance
- Establish an Insider Threat Program
- Establish an Insider Threat group (program personnel) from offices across the contractor's facility, based on the organization's size and operations
- Conduct self-inspections of Insider Threat Programs
- Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees
- Monitor classified network activity

REFERENCES

- **32 CFR Part 117** – National Industrial Security Program Operating Manual (NISPOM)

ESTABLISHING AN INSIDER THREAT PROGRAM (ITP) BEST PRACTICES: PHASES

EVALUATION PHASE

- Need and purpose for Insider Threat Program (ITP) articulated
- Build consensus and advocacy among core stakeholders
- Identify senior executive buy-in for Implementation Plan
- Executive Order/Policy for ITP Implementation Plan
- Assignment of responsibility for program oversight and development
- Identify and review historical Insider Threat incidents
- Consider the threat environment to include technologies heavily targeted by adversaries and the threat of foreign recruitment of insiders with access to these technologies
- Consult **DCSA Counterintelligence Directorate** publications and your local DCSA Counterintelligence Special Agent for applicable threat information
- Review regulatory compliance requirements
- Review prior risk assessment documentation

FORMULATION PHASE

- Risk management processes initiated to identify assets, threats and vulnerabilities
- Define Protection Specification (people, assets, property, systems)
- Policies and procedures are written to support the development and operation of all ITP elements
- Identify requirements for core elements: Operations, Analytics, Collaboration, and Education
- Incorporate counterintelligence controls and measures
- Incorporate security controls and measures
- Incorporate Information Security controls and measures
- Incorporate human resources data
- Determine technologies for monitoring and analytics
- Formulate incident response requirements
- Ensure sound reporting procedures
- Self-Inspection and improvement requirements incorporated
- Completed ITP Implementation Plan is reviewed and approved by senior management official

IMPLEMENTATION PHASE

- High-level, company-wide policies are written, approved, and published
- ITP is formally launched and is operational

ESTABLISHING AN INSIDER THREAT PROGRAM BEST PRACTICE: CORE ELEMENTS

1. **Operations Management & Planning:** refers to the Implementation Plan, leadership, policy creation, legal and privacy review, plan development, implementation, and administration of the core program elements. This element includes support of the ITP program by senior leadership at the facility.

2. **Gather**: refers to the processes of gathering information and evaluating it to determine the appropriate reporting channels. In this process you will create and maintain an inventory of behavioral indicators associated with Insider Threats. You will also define metrics to evaluate performance. This process helps to reduce false positives and improves identification rates. It also provides guidance for monitoring strategies and informs senior leadership.

3. **Collaboration**: refers to the use of internal and external relationships to facilitate the acquisition, sharing and reporting of information potentially indicative of Insider Threat behaviors and activities.

4. **Education**: refers to the processes associated with Insider Threat education, training, and awareness programs apportioned appropriately with the basic, intermediate, and advanced program models.

5. **Protection Specification**: refers to risk assessment processes aimed to identify assets, competitive and threat landscape, vulnerability analysis, legal liability, security implications to business viability, profitability, reputation, and personal safety.

6. **Counterintelligence**: refers to a programmatic approach to the identification, disruption, neutralization, and mitigation of Insider Threats.

7. **Monitoring**: refers to the designation and implementation of manual or automated technical monitoring technologies, processes, and protocols essential for the accomplishment of the program objectives delineated in the respective model: basic, intermediate, or advanced.

8. **Incident Response**: refers to the procedures and protocols to respond to technical and non-technical indicators, incidents, and events. Procedures will be implemented to direct and indirect interventions, investigations, and other similar follow-up.

9. **Audit & Improvement**: refers to review and audit management processes required to assure that the program is operating pursuant to plan, identifies lessons learned, and implements improvements based on metrics and other analysis.

MONITORING CLASSIFIED NETWORK ACTIVITY GETTING STARTED: KEY ELEMENTS

Audit records will include the following:

- Enough information to determine the action involved, the date and time of the action, the system on which the action occurred, the system entity that initiated or completed the action, and the resources involved (if applicable);
- Successful and unsuccessful logins and logoffs;
- Unsuccessful accesses to security-relevant objects and directories;
- Changes to user authenticators;
- The blocking or blacklisting of a user ID, terminal, or access port;
- Denial of access from an excessive number of unsuccessful login attempts

In addition to the above security-relevant system events, audit records will be maintained for the activities listed below. A single record or log may document multiple types of activities, such as:

- User briefing statements
- Additions, deletions, reconfiguration, and repair actions to accredited hardware
- Installation, modification or testing of operating system and security related software
- Actions taken to sanitize IS components
- The placement and destruction of security seals

A review of all IS audit records will be performed in accordance with the guidance outlined in the DCSA Process Manual. If analysis of the audit records reveals unauthorized actions that are not easily explained, the details will be reported to the ISSM for review and further action as necessary. Any incident that involves suspected compromise of classified information will be immediately reported to DCSA.

ISSMs may choose to install and use audit reduction tools on larger or high-traffic systems. Audit reduction tools are considered security relevant and must be evaluated by the Information Security System Professional (ISSP). Raw audit trails will be retained for the system to provide data for analysis in the event of an inquiry or investigation into an IS related event.

Guidelines for reviewing automated audit records:

- Review and verify there have been no changes to system time and that the automated audit functions are performing properly. Review BIOS changes and other configuration changes not identified in the SSP.
- Review all failed logins. Question multiple failed login attempts and account lockouts
- Review a sampling of successful logins to ensure those persons were actually present and using their account during the recorded time periods. For example, if you are aware of someone being on

travel or on vacation during the week, verify his or her account was not accessed.

- Question login sessions that occur at unusual times (e.g., 2:00 a.m.) or sessions that are left open for long periods of time.
- Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the (M)SSP.
- If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs.
- Depending on the available audit mechanism, failed attempts to access objects may be all inclusive rather than limited to security-relevant objects. Attempt to focus your review on identifying any user ID that consistently has failed access attempts to privileged system files.

GATHER

It is not enough to simply monitor and collect data/information. To be useful, the data/information must be gathered and evaluated to detect potential or actual Insider Threats and reported to the FSO and DCSA. Two common methods of gathering data/information are manual and automated.

- **Manually** gathered data/information relies on analysts or program personnel for review. The program is reliant on the skills of the analysts involved and is often less expensive than automatic processing options, although the number of users and the amount of data being collected may require several analysts, resulting in higher costs.
- **Automated** data/information gathering relies on algorithms to scan data, which streamlines the discovery of adverse information; however, this type of automatic processing is expensive to implement.

Gathered information may be derived from system monitoring, but also integrated with data/information from security incidents or violations, human resources or personnel information, or any other items that impact the status of the facility clearance, the status of an employee's personnel security clearance, that may indicate the employee poses an Insider Threat, that affects proper safeguarding of classified information, or that indicate classified information has been lost or compromised.

REPORTING

- Reporting refers to the actions taken by employees to inform the Insider Threat Program of actual or suspected insider threat activities and indicators.
- Reporting is the culmination of the metrics and information derived from integrating and gathering collected data/information and is an essential component of any Insider Threat Program. Reporting considerations include weighing the pros and cons of real-time versus event-triggered monitoring.
- Real-time monitoring, while proactive, may become overwhelming if there are an insufficient number of analysts involved.
- Event-triggered monitoring is more manageable because information is collected and reported only when a threshold is crossed; however, because event-triggered monitoring is reactive, it typically operates behind the threat, leaving open an opportunity for increased damage.

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.

INSIDER THREAT PROGRAM FOR INDUSTRY JOB AID