Carnegie Mellon University
Software Engineering Institute

Insider Threat Program Evaluation (ITPE)

Capability Questions and Indicators

Workbook: Personnel and Training

https://www.sei.cmu.edu

Design: REV-03.18.2016.0 | Template: 01.04.2023

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0883

Table of Contents

Introduction

The insider threat program evaluation (ITPE) was developed by staff in the CERT® Division at the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) at Carnegie Mellon University. The evaluation, which is based on the National Insider Threat Task Force (NITTF) minimum standards[1] and Federal mandates for insider threat programs, along with other sources of best practices, enables organizations to gain a better understanding of their insider threat program (InTP). The evaluation was designed to be completed over a period of three to five weeks, with a few weeks of planning and information gathering that occurs before week one. Week one is the pre-evaluation week, where evaluation team members review organization-supplied documents to become familiar with organization practices and policies. During week two, the evaluation team spends three to five days onsite at an organization. During that time, the evaluation team reviews documents, interviews key personnel, and observes processes to substantiate each capability. During the final weeks, the evaluation team prepares an insider threat program evaluation final report, describing how prepared an organization is to manage insider threats.

According to the NITTF minimum standards, "Insider threat programs are intended to: deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative or other response actions…"

The ITPE takes into account the minimum standards required for federal agencies, which focus on insider threat programs for classified information systems and networks. However, it also includes a broader set of best practices for all types of organizations as well as best practices for non-classified systems and networks.

This workbook, Personnel and Training, evaluates the make-up of the organization's insider threat program and team to ensure all the right organizational components are involved. It also measures the comprehensiveness of the insider training provided to employees, trusted business partners, and the insider threat program team members. The evaluation looks for evidence of role-based training, training for managers and supervisors on recognizing at-risk employees and providing proper assistance, and also for training for those handling sensitive or classified materials.

Indicators within capabilities that are marked with a "[NITTF]" at the sentence end, mean that the indicator came from the NITTF minimum standards. In addition, those indicators that include

® CERT® is a registered mark owned by Carnegie Mellon University.

[1] Authority for the minimum standards comes from Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; Executive Order 12968, Access to Classified Information; National Policy on Insider Threat.

"[NISPOM]" are also those required to meet National Industry Security Program (NISPOM[2]) standards. Those preceded by "[For U.S. Federal Government Only]" mean that the indicator only applies if the organization being evaluated is a U.S. Federal Government agency or department, if not then those indicators should not be evaluated or included in the scoring.

[2] National Industry Security Program (NISPOM) Operating Manual February 2006, with Change 2, May 2016 incorporated. DoD 5220.22-M

Generic Clarifications

For the purposes of this assessment, the following simple definitions and distinctions are used:

- Policy – the rules, guidelines, laws, or regulations that govern or constrain operations
- Process – describes "what happens" (or "what to do")
- Procedure – describes "how-to" or step-by-step instructions that implement the process
- Practice – the set of policies, processes, procedures, and activities that are followed

An insider is defined as any person who supports the organization, including employees, and trusted business partners.

A malicious insider is a current or former employee, contractor, or other business partner who

- has or had authorized access to an organization's network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

An unintentional insider is a current or former employee, contractor, or other business partner who

- has or had authorized access to an organization's network, system, or data
- through their action/inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Trusted business partners include contractors, sub-contractors, supply-chain partners, vendors, and other similar entities.

Organizational staff are the internal staff of the organization being assessed.

A data owner is an individual with full custodial and administrative rights over a given set of data. The data owner can authorize or deny access to certain data and is responsible for its accuracy and integrity.[3]

[3] From www.businessdictionary.com/definition/data-owner.html

2.1 Organization-Wide Participation

Participation in the InTP is organization-wide.

Clarification/Intent

A key tenet of establishing an InTP is to ensure the organization is widely represented. Main areas that should be involved in the planning, design, implementation, and operation of an InTP should include staff with expertise in the areas of IT, Legal, Human Resources, Personnel and Physical Security, and Counterintelligence where applicable. Others with expertise in contracting and/or finance and data protection and architecture may also be involved. Because participants come from a wide variety of backgrounds and experiences, communication and coordination must be established and effective.

Evaluation Team Guidance

Participants in the InTP may be full-time or part-time members of the actual InTP team or individuals who are considered subject matter Experts (SMEs) who are called upon as needed. In addition to the InTP team, the structure of the InTP can vary. There may be an insider threat program council or working group comprising senior leaders of key business lines (CIO, CSO, Legal Counsel, etc.) who help the InTP leader identify and gain access to data sources, and assist in development of the team charter, policies, procedures, and other guidance. Once the InTP program is fully functional, this council may become more ad-hoc in nature or take on an oversight role.

When evaluating the organizational participation, those roles that are listed in Level 2 – match the roles identified by the NITTF minimum standards; along with a few based on CERT research. Those in the levels 3 and 4 come from best practices identified through research by the CERT Insider Threat Center or other similar experts.

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE.

- What parts of the organization are involved in the insider threat program (including their responsibilities or roles and the actions they perform)?
- Which group has the lead for the Insider Threat Program?
- How do the groups coordinate with each other?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Components of the organization participating in the InTP include

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ Senior leadership

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Human Resources (HR)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Information Technology (IT)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Security group (if separate from IT)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ Cyber security or information assurance group (if separate from IT)

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Legal Counsel, including civil liberties and privacy

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Physical Security or Facilities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Law Enforcement or liaison with law enforcement

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Personnel security or counter Intelligence (if applicable) or other investigative group

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Behavioral Sciences or similar group

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Activities between groups are coordinated appropriately.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ There are defined roles and responsibilities for all participants.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Components of the organization participating in the InTP also include

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Acquisitions/Contracts/Purchasing

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Financial

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A list of all participants who require background checks has been established.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ All participants who require background checks and other vetting activities have been so vetted before they begin performing their duties.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ All participants with access to classified, sensitive or intelligence information have been thoroughly vetted and trained.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Defined processes and communication channels are in place for coordinating activities between groups.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ An Insider Threat Council or Working Group has been established to help guide the development and implementation of the InTP.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Components of the organization participating in the InTP also include

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ Lines of Business (product, service, and data owners)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Union representation (if applicable)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ The Insider Threat Council or Working Group continues to function after the InTP has been implemented, on a persistent basis.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

2.2 InTP Team Composition

The InTP team is composed of team members with the appropriate skills and abilities.

Clarification/Intent

The InTP team may perform but is not limited to the following activities: performs the day-to-day functions of the InTP, conducts centralized analyses on aggregated organizational data sources to detect insider threat anomalies, uses the organization's data sources to support allegation resolution, reports on insider threat trends and future threats, involves subject matter experts as needed, and passes on information to organizational units responsible for investigations and inquiries. The InTP may also have only a core set of active members, such as IT, information assurance, HR, physical security, and legal, with others being participants. The InTP team member responsibilities will vary, but they can include the following:

- Senior executives are visible advocates and provide necessary policies.
- InTP team lead manages day-to-day operations, develops the team charter and procedures, manages the budgets and resources, makes final decisions, and reports to senior management.
- Data analysts perform the day-to-day operations of the team, review alerts and reports to determine anomalous or suspicious behavior and determine if it requires further investigation.
- Cybersecurity specialist, also known as an Information Security Specialist, has in-depth knowledge and understanding of the cyber tools, tactics, and techniques used to protect an organization's IT infrastructure. This specialist knows what data is collected by information assurance tools and can provide recommendations for how to configure cybersecurity tools to meet InTP needs.
- Data architect knows where data is and its rules of access/use and can provide relevant information on data acquisition, analysis, protection, and retention.
- Senior technologist analyzes technologies and makes recommendations for their acquisition, use, adaptation, or modification in support of the InTP.
- HR specialist knows all of the data and processes of HR, when insider threats need to involve HR, and can help create and implement insider-threat-related HR policies and procedures.
- Financial specialist knows what financial data is collected, processed, and stored and how to handle that data in support of insider threat anomaly detection and resolution.
- Legal specialist advises the team manager, reviews proposed policies and procedures, and ensures compliance with relevant standards, regulations, and laws, especially privacy and civil rights.
- Behavioral science specialist provides context to the team by identifying and evaluating observed behaviors or artifacts of behavior in data for potential anomalies and allegations.
- IT support builds, operates, and maintains InTP infrastructure and tools and should include a computer systems engineer, system administrator, database administrator, interface designer, network architect, and algorithm specialist.
- Counterintelligence (if applicable) is knowledgeable about and experienced with CI investigations and analysis.

Evaluation Team Guidance

When evaluating the InTP team, note that staff DOES NOT have to be full-time, they can participate part-time or as SMEs when needed.

In Level 4 the third indicator states "The InTP interfaces with any internal fraud group if such a group exists in the organization." This indicator may only be applicable to financial services organizations but it is possible that there are other organizations that have internal fraud groups. Specifically in financial services organizations there may also be an internal watch group looking for insider trading. Many InTP groups in industry do not include fraud within their scope because of these other specific groups. However, some acknowledgement of both groups by the other is a best practice to ensure there is not data that will need to be shared between the groups or other assistance that can be provided between the groups. The internal fraud group could be considered part of the broader InTP even if the InTP core team does not handle fraud events or incidents, and even if the internal fraud group has its own authority. The two could work together with separate roles and responsibilities. This particular indicator is looking to ensure that the InTP knows about any internal fraud groups within its organization and also has established, with management approved, communications or information sharing where appropriate. Such an internal fraud group may also need to be included in any working group or council.

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE:

- What different types of personnel are on the InTP team?

- How will staff in other locations or countries be assigned roles for data collection and analysis, training, and the prevention, detection, and response to insider threats?
- How are they prepared to perform their jobs?
- Are there any internal fraud groups within your organization? Does your InTP interface with them? What type of interaction is done? Are they considered part of the InTP?
- What type of surge support or reachback capability exists for the InTP during large incidents or crises?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ A designated InTP team is established. [Note: The team does not have to have the name InTP team.]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP team members should include (as full time, part time, or SMEs, as applicable) the following roles.

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ Team manager or lead

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Data analysts

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Cybersecurity specialist

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ HR specialist

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Personnel security or counterintelligence (if applicable)

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Legal specialist

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Behavioral science specialist

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Information technology support

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Physical Security or Facilities support

Doc Rev _____

Dir Obs _____

Intvw _____

☐ All team members have defined roles and responsibilities.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP team has the assigned authority commensurate with its responsibilities.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ InTP team members include the following roles (as full time, part time, or SMEs, as applicable):

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ Data architect or similar role

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Senior technologist

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Financial specialist

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ Contracts, Acquisition, or Purchasing support

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ Sufficient personnel for day-to-day functions and operations are assigned to the InTP team.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Reachback personnel or resources for surge efforts are in place.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Processes are in place to handle activities involving geographically dispersed team members.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP incorporates or works in conjunction with any established workplace violence program.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP interfaces with any internal fraud group if such a group exists in the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

3.1 Insider Threat Awareness Training for Organization

The appropriate levels of insider threat awareness training are provided for all organizational personnel.

Clarification/Intent

The basic level of training and awareness should be available to all employees, including managers, supervisors, C-level and executive managers, trusted business partners, contractors, supply chain collaborators, members of the InTP Team (InTP) and Council. Awareness training can also include web sites with appropriate information available to any employee.

Evaluation Team Guidance

Insider threat awareness training can be in-person or computer-based.

In Level three the second indicator states "The InTP is publicized and promoted in the general security awareness training." There is a caveat to this indicator, if the InTP has decided to keep its program confidential, then this indicator is Not Applicable and should be marked as such. If the InTP has decided to only make some of its program public to its employees then this indicator is met if that portion is indeed publicized.

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE:

- How would employees on foreign travel know what to do to protect themselves if approached with a job offer from a foreign government?
- What would employees do if they received an email from the SOC asking them to change their password through a link in the email?
- What explanation is given if an employee asks what insider activity is?
- What type of training is given to new hires about information security and insider threats?
- How would staff be trained to handle a classified or sensitive data spillage?
- What assistance is provided to employees if they ask why someone would target them as part of malicious insider activity?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Yearly employee insider threat awareness training is provided for all employees. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Yearly employee insider threat awareness refresher training is provided for all employees. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Awareness training and refreshers cover

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ types and indicators of insider behavior [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ adversarial methodologies to target and recruit employees in order to collect information or gain access [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ unintentional insider threats

Doc Rev _____

Dir Obs _____

Intvw _____

☐ the importance of detecting and reporting suspected insider threat activity [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ insider threat reporting mechanisms, processes, and procedures [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ counterintelligence and security reporting requirements as applicable [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ foreign intelligence/competitor elicitations

Doc Rev _____

Dir Obs _____

Intvw _____

☐ separation of duties

Doc Rev _____

Dir Obs _____

Intvw _____

☐ acceptable organizational behavior and violations

Doc Rev _____

Dir Obs _____

Intvw _____

☐ insider threat program policies

Doc Rev _____

Dir Obs _____

Intvw _____

☐ An internal network site has been established and promoted to all employees to provide access to insider threat reference material. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Reference materials address topics covered in the awareness training. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ There is training to address classified and sensitive data handling and counter intelligence, for staff handling such data, if applicable.[NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Employees are made aware of their organizational responsibility to report anomalous or suspicious behavior. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government and Government Contractors Only] Training occurs within 30 days of employment or granting access to classified or sensitive data or networks. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training completion is tracked and verified. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ General security awareness training addresses advanced topics such as social engineering, unintentional data leaks, and social media.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP is publicized and promoted in the general security awareness training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Staff are assigned to manage and coordinate training across all levels of the organization.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Insider threat awareness training includes ongoing activities, such as randomly conducted exercises that test an employee's knowledge of insider threat or how to react in certain situations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training effectiveness is evaluated and changes made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Trusted business partners receive the same insider threat awareness training and refreshers as organizational staff.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

3.2 InTP Team Training

Members of the InTP Team receive detailed training to enable them to handle their roles and tasks effectively.

Clarification/Intent

All members of the InTP Council and InTP Team receive core training so that they understand the following:

- Roles and responsibilities—to ensure they perform their mission properly
- Authority (if any)—to ensure they are not acting outside of their scope of authority
- Constraints or limits of their authority or responsibilities—to ensure they are clear on what they can and cannot do, especially in regard to legal, civil liberties, and privacy issues
- Policies and methods for storing and protecting data—to ensure that all data collected is properly safe-guarded
- People with whom they can and cannot share data—to ensure data is protected and shared only with authorized personnel
- Appropriate escalation chains—to ensure they understand where they should refer issues and incidents

Training for processes and procedures relates to those used to collect and analyze technical and behavioral data, specific tools depending on their roles, triggers and indicators for potential or ongoing insider threat, key assets that must be protected, new methods of attack, new detection and mitigation strategies, and new research in the area of insider threat. Training for legal aspects should include federal, state, and local laws and regulations concerning civil liberties and privacy, what type of monitoring is considered valid and legal, and the types of wording that must be in contracts, non-disclosure agreements, and IP agreements.

Evaluation Team Guidance

Most organizations with access to classified systems already have a detailed training program in place to ensure that only staff with acceptable clearances and proper training can use such systems. Existing training should include how insiders have performed malicious actions on classified systems and the corresponding impacts. Staff with access to such systems should be taught how and why they may be targeted and indicators to watch for in coworkers.

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE:

- What type of training and materials does each stakeholders in the insider threat program receive?
- What type of training do new hires receive about information security and insider threats?
- What training do HR and Legal staff receive regarding insider threat activities and how to handle them?
- What type of training do InTP team members receive?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Insider threat program staff/team training is provided and covers

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ roles, responsibilities, and authority of InTP team

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ daily operational processes and procedures for the InTP team functions [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including consequences of misuse of such information [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ handling and sensitivity of data collected by the InTP [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ communication and escalation of insider threat events or activities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ organizational procedures for conducting insider threat investigations and response actions [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ conflict of interest, especially as it relates to investigations

Doc Rev _____

Dir Obs _____

Intvw _____

☐ applicable civil liberties, privacy laws, regulations, and policies [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ user monitoring policy and appropriateness

Doc Rev _____

Dir Obs _____

Intvw _____

☐ counterintelligence and security fundamentals including related legal issues (as applicable) [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government Only] Investigative referral requirements of Section 811 of the Intelligence Authorization Act for FY 1995 as well as other policy or statutory requirements regarding referrals to an internal entity such as security officer or Office of Inspector General, or external investigative or law enforcement entities (FBI, DoJ, etc.) [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training completion is tracked and verified.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Classified and sensitive data handling training is provided for cleared personnel.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Assigned staff manage and coordinate training of the InTP Team.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Training for InTP includes ongoing activities, such as randomly conducted exercises or scenarios that test the team's knowledge of how to handle insider threat events and react to certain situations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP staff are readily approved to take the required insider threat training (defined in level 2 above) and provided the time needed to attend the training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP staff are readily approved for at least yearly professional development activities related to their InTP roles, responsibilities, individual development plans or key performance indicators.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training effectiveness for InTP team is evaluated and changes made as necessary.

Doc Rev

Dir Obs

Intvw

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

3.3 Role-Based Training For Organization

The appropriate levels of role-based training are provided to staff performing InTP or related activities.

Clarification/Intent

Role-based training for different parts of the organization that might have to handle tasks or events related to insider threat prevention, detection, and response should be established and tracked for all relevant employees and trusted business partners.

Evaluation Team Guidance

Relevant organizational staff who may require such training might include those

- within HR, responsible for hiring, orientation, performance reviews, employee separation, employee counseling
- within Legal areas related to regulations or policies involving hiring, performance reviews, employee separation; IP, acceptable use, and non-compete policies; NDAs and contracts; or investigations, privacy, and civil liberties
- within IT or cybersecurity areas related to acceptable use, data exfiltration controls, logging and audits, or network traffic collection and analysis
- within physical security
- within personnel security or counterintelligence if appropriate

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE:

- What parts of the organization receive any customized insider threat prevention, detection, or response training?
- What type of training about insider threat behaviors and how to prevent, detect, or respond to them, do the following staff receive?
  - HR staff
  - Legal staff
  - Physical security staff
  - Counterintelligence or personnel security staff (as applicable)
  - Contracts and Procurement staff
  - IT staff
- Who provides this training?
- What kind of refresher training is given?
- Are any exercises or scenarios conducted?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Specific roles that require role-based insider threat training are identified.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training required for each role is developed and provided.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Refresher training required for each role is developed and provided.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Role-based training and refreshers cover

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ indicators of insider threat behavior that various roles may come across in their daily duties

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ methods for identifying potential or actual insider threats

Doc Rev _____

Dir Obs _____

Intvw _____

☐ processes for reporting suspected or actual insider threat behaviors or activities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ persons to contact for assistance or additional information

Doc Rev _____

Dir Obs _____

Intvw _____

☐ applicable civil liberties, privacy laws, regulations, and policies

Doc Rev _____

Dir Obs _____

Intvw _____

☐ communication and escalation of insider threat events or activities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ organizational procedures for conducting insider threat investigations and response actions

Doc Rev _____

Dir Obs _____

Intvw _____

☐ methods for prevention of insider threat activities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ insider threat program policies

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training completion is tracked and verified

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Staff are assigned to manage and coordinate role-based training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Curriculum for each role is developed.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Role-based training includes ongoing activities, such as randomly conducted exercises or scenarios that test the staff's knowledge of how to handle insider threat events and react to certain situations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Staff are readily approved to take required role-based training and provided the time needed to attend the training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training effectiveness for role-based training is evaluated and changes made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)

3.4 Manager and Supervisor Training

Training is provided to managers and supervisors regarding prevention, detection, and response to insider threat behaviors and events.

Clarification/Intent

Specific role-based training is required for organizational supervisors and managers. Such training may include complying with all organizational policies and procedures related to insider threat detection and mitigation; assessing trustworthiness of employees; identifying potential behavioral precursors to malicious insider activities; identifying employees under stress and helping them get the right counseling or assistance before they act; and managing and coaching employees to help them achieve their best performance.

Evaluation Team Guidance

Training should also include awareness of other similar programs such as workplace violence, protection of whistleblowers, and employee assistance programs.

The following open-ended questions can be used to get the conversation started or to introduce this particular capability to set the stage for the ITPE:

- How would a manager or supervisor know how to recognize potential insider threat behaviors?
- How would a manager or supervisor know how to recognize an employee at risk or under stress?
- What resources are managers or supervisors provided to enable them to assist at-risk employees?
- What type of management and leadership courses are provided on a regular bases to help managers and supervisors create a fair and open work place?
- Who provides this training?
- What type of refresher training is given?
- Are any exercises or scenarios conducted?

Agency Response

Evidence Sought

Auto Verification

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Management and supervisory training is provided for all managers and supervisors so they can identify potential employee problems, handle problems, and assist employees.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Required refresher training is developed and provided.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Manager and supervisory training and refreshers cover

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ recognizing employees at risk or under stress

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ providing assistance or referrals for employees at risk or under stress

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ recognizing precursors of insider threat behavior

Doc Rev

Dir Obs

Intvw

☐ indicators of insider threat behavior

Doc Rev

Dir Obs

Intvw

☐ methods for identifying potential or actual insider threats

Doc Rev

Dir Obs

Intvw

☐ processes for reporting suspected or actual insider threat behaviors or activities

Doc Rev

Dir Obs

Intvw

☐ whom to contact for assistance or additional information

Doc Rev

Dir Obs

Intvw

☐ applicable civil liberties, privacy laws, regulations, and policies

Doc Rev

Dir Obs

Intvw

☐ communication and escalation of insider threat events or activities

Doc Rev

Dir Obs

Intvw

☐ organizational procedures for conducting insider threat investigations and response actions

Doc Rev

Dir Obs

Intvw

☐ methods for prevention of insider threat activities

Doc Rev

Dir Obs

Intvw

☐ insider threat program policies

Doc Rev

Dir Obs

Intvw

☐ Training completion is tracked and verified.

Doc Rev

Dir Obs

Intvw

Level 3

☐ Manager and supervisory training and refreshers also cover

Doc Rev

Dir Obs

Intvw

☐ managing and coaching employees to help them achieve their best performance

Doc Rev

Dir Obs

Intvw

☐ assessing trustworthiness of employees

Doc Rev

Dir Obs

Intvw

☐ Staff are assigned to manage and coordinate management and supervisory insider-threat-related training.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Manager and supervisory training includes ongoing activities, such as randomly conducted exercises or scenarios that test their knowledge of how to handle insider threat events and react to certain situations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Managers and supervisors are readily approved to take required role-based training and provided the time needed to attend the training.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Training effectiveness for insider-threat-related manager and supervisory training is evaluated and changes made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

Score: ☐ **Not applicable** ☐ **1** ☐ **2** ☐ **3** ☐ **4**

Justification

Evidence Collected					
Document Review		**Direct Observation**		**Interview**	

Notes (from documentation, observations, and interviews)