Carnegie Mellon University
Software Engineering Institute

Insider Threat Program Evaluation (ITPE)

Capability Questions and Indicators Workbook: Program Management

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. Week one is the pre-evaluation week, when evaluation team members review organization-provided documents to become familiar with organization practices and policies. During week two, the evaluation team spends three to five days on-site at an organization. During that time, the evaluation team reviews documents, interviews key personnel, and observes processes to substantiate each program 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, Program Management, measures how well an organization establishes, manages, and governs its InTP. It uses as a baseline all the things that the NITTF says should be in place to show the program is formal and supported, such as an insider threat policy defining the program, a designated senior leader, and communications and incident response plans. It uses CERT Insider Threat Center best practice research and analysis for many of the other required baselines and the other scoring levels.

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 "[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

® 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.

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

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.

Generic Clarifications

For the purposes of this evaluation, 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 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

1.1 Formalized Program

A formal Insider Threat Program has been established.

Clarification/Intent

An insider threat program helps an organization deter, detect, and respond to an insider incident. A comprehensive InTP begins with a formalized InTP team that includes decision makers and experts from different teams across the organization. By implementing an InTP, the organization can be prepared to handle an insider threat in an effective, confidential, and timely manner.

An InTP also helps organizations to develop processes and techniques that can help proactively detect anomalies that indicate that an employee may turn into a malicious insider. All insiders could pose a threat, some more than others. Leveraging this proactive, observable-based approach helps an organization prevent, detect, and respond to the threat before an insider commits his or her activity.

Managing insider threats is an essential component of an enterprise risk management program (ERP). If there is no ERP, one must be created along with the InTP.

A financial plan and budget for the InTP is needed to ensure sustainment and resilience for the program. If the program is not fully operational, there must be an implementation plan that addresses standing the program up.

Evaluation Team Guidance

Each organization should work side-by-side with Legal Counsel, Privacy Officers, and other representatives from across the organization to build its program. Members of organizational management, the Insider Threat Program (InTP) team, and governance groups such as an InTP council or working group must be familiar with privacy laws, civil liberties laws, and existing legal mandates, statutes, and directives related to implementing an InTP. This familiarity helps to ensure that the program meets all legal requirements and actions, such as those related to user monitoring, confidential reporting, and protecting employee rights. Relevant laws include but are not limited to the Bill of Rights, the Privacy Act of 1974, the Electronic Communications Privacy Act, the Rehabilitation Act of 1973, Title VII of the Civil Rights Act of 1964, civil liberties principles, and prohibited personnel practices.

For companies and organizations operating in multiple countries or jurisdictions, the legal and other challenges posed by the differing laws, regulations, and applicable standards call for inclusion of legal, privacy, and HR Subject Matter Experts (SMEs) from those other countries or jurisdictions in the establishment of the InTP and its policies and procedures.

Note that NISPOM requires that when there is a corporate-wide InTP with a designated senior officer, each legal entity, or separate division, of the company using the corporate-wide InTP services must declare that the overall corporate-level senior official is also their (the legal entity's) designated senior official for InTP.

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:

- Who is involved in the InTP?
- Who manages or leads the InTP group?
- How was authority for the InTP announced and institutionalized?
- How does management show support for the InTP?
- How does management talk or engage with employees about the InTP?
- What types of insider threats and activities is the InTP meant to address?
- How is the InTP funded in the short and long term?
- If there are multiple locations:
  - How will the InTP be implemented across the different sites and countries?
  - How will staff from other locations participate in data collection and analysis, training, and the prevention, detection, and response to insider threats?

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

☐ The organization has established a program for preventing, detecting, and mitigating insider threat behavior and action (i.e. a formal InTP) for classified (where applicable) and unclassified networks, systems, and information.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP includes but is not limited to [NITTF] [NISPOM]:

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ assigned staff and SMEs to perform InTP activities and functions

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ defined authority commensurate with assigned responsibilities

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ an integrated capability to monitor and audit information (including user monitoring) to detect and mitigate insider threats

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ policies and procedures for sharing information across counterintelligence, security, information assurance, and HR (as applicable)

Doc Rev _____

Dir Obs _____

Intvw _____

☐ training for InTP staff and all organizational employees

Doc Rev _____

Dir Obs _____

Intvw _____

☐ confidential reporting capability to report suspicious or anomalous behavior

Doc Rev _____

Dir Obs _____

Intvw _____

☐ centralized analytical and reporting capabilities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ an identified response capability and process

Doc Rev _____

Dir Obs _____

Intvw _____

☐ established mechanisms for oversight and management support

Doc Rev _____

Dir Obs _____

Intvw _____

☐ established mechanisms for evaluating the program

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP has a documented charter or CONOPS that defines its mission, functions, and operations.

Doc Rev

Dir Obs

Intvw

☐ Designated senior leadership has the authority and accountability to manage, provide resource recommendations, and provide oversight for the InTP. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ The senior official designated to establish and execute the InTP shall be cleared in connection with the facility and shall also be the Facility Security Officer (FSO) or shall ensure the FSO is a member of the InTP implementation program. [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ A corporate family that establishes a corporate-wide InTP with one designated senior official to establish and execute the program must designate that senior official as the InTP Senior Official for each cleared legal entity using the corporate program. [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ The InTP has been developed and implemented in consultation with legal, civil liberties, and privacy officials. (For federal agencies, legal officials should include General Counsel.) [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ InTP activities are conducted in accordance with applicable laws, whistleblower protections, civil liberties and privacy policies. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ The InTP has a yearly budget.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government Only] The InTP designated senior official has submitted to the agency head an implementation plan for establishing an InTP. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The InTP has been announced to the organization to the extent possible or appropriate.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP has visible senior and executive management participation and support (e.g., newsletters, meetings, memos)

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP has a five-year financial plan.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP has a defined process for keeping up with changes in laws and regulations pertaining to insider threats, privacy, civil rights, etc.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP includes capabilities for preventing, detecting, and mitigating insider threat behavior and action (i.e., a formal InTP) for classified (where applicable) and unclassified facilities and physical security incidents.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The InTP includes capabilities for preventing, detecting, and mitigating insider threat behavior and action (i.e., a formal InTP) for classified (where applicable) and unclassified facilities related to workplace violence including active shooters (if appropriate).

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)

1.2 InTP Policy

A formal InTP policy has been established and institutionalized.

Clarification/Intent

The InTP policy should institute the InTP and the organization's view of what is considered insider threat behavior.

It should define the InTP's

- leadership
- authority
- scope
- mission
- functions

It should also articulate the organization's definition of

- who is considered to be an insider
- what is considered to be an insider threat
- what is considered to be insider threat behavior
- how such behavior is reported
- the consequences for performing such behavior

For federal agencies, this policy and its supporting procedures and guidance should be driven and managed by the designated senior official. For all organizations, it should be developed with assistance by legal and privacy officers and be executed in accordance with all applicable laws and regulations.

Evaluation Team Guidance

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 types of insider threats and activities are the organizational program meant to address?
- How is the InTP documented?
- If there is a formal InTP policy, what does it cover?
- What facilities and sites are covered by the InTP policy?

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

☐ An approved, organization-wide insider threat policy exists and is applicable to all organizational personnel. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The insider threat policy is approved by the organization head. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. federal government only] Agency policies shall include internal guidelines and procedures for the implementation of the NITTF minimum standards. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP policy includes guidance and procedures that define the goals, components, operation, and implementation of the program.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The insider threat policy was developed in conjunction with legal, data retention, civil rights/liberties, and privacy officials. (For federal agencies, legal officials should include General Counsel.) [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The InTP policy has been made available to employees within the organization to the extent possible or appropriate.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP policy or a supplemental document defines the scope of the program, including but not limited to

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ types of insider threats to be addressed

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ organizational assets that must be protected

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ types of data to be collected and analyzed (general sources, does not have to be specific sources)

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ personnel to be involved in the InTP

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ sites and facilities that are bound by the policy

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ the consequences of performing malicious or unintentional insider threat actions

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Violations of InTP policies are addressed.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Groups from across the organization (e.g., IT, security, HR, Legal, financial, lines of business, and where applicable, unions) helped to develop InTP policies and procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A process is in place for developing, approving, communicating, updating, and retiring InTP policies and related procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Policies and procedures are periodically evaluated for effectiveness and corrected as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP policies and procedures are coordinated with other organizational policies and procedures to resolve conflicts, eliminate redundancies, and increase efficiencies.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ An approved insider threat policy exists that applies to trusted business partners.

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)

1.3 Insider Threat Response Plan

A set of documented and maintained plans exists governing the response capability for insider threat events.

Clarification/Intent

An InTP requires a well thought-out, documented, and practiced response plan and supporting procedures. These procedures must

- ensure that a response is repeatable, standardized, and applied consistently
- comply with all legal, ethical, privacy, and civil liberties requirements

The insider threat incident response plan should include how incidents perpetrated by insiders are

- detected
- reported
- contained
- remediated
- documented
- prosecuted (if applicable)

The response plan should tie into and support any communication plan for organizational or insider-threat events. The response plan should define the process for

- escalation
- notifying management and other stakeholders
- handoff to investigations unit or law enforcement

Various resolution actions can be involved in the response process. These can include but are not limited to

- Internal response options
    - retraining
    - personnel actions
    - organizational sanctions
    - legal actions
- External response actions
    - referral to internal investigative unit or counter intelligence (if applicable)
    - referral to local or federal law enforcement if applicable

A postmortem review of how a particular event or incident was detected and handled through resolution should be considered following an insider threat incident against high-value targets/assets, a situation that went very well, or a situation that did not go very well. The insider incident response plan should be periodically tested; this can include mock incident scenarios to test processes against new threats or situations that have not yet occurred or table top exercises with situations developed by team members or pulled from the newspaper. Improvements should be planned and implemented based on feedback and lessons learned.

Evaluation Team Guidance

Organizations must be ready to respond to an incident involving malicious or unintentional insider threats at any time. Some organizations use their existing incident response plans for insider threats. These plans typically include additional elements to ensure that confidentiality, privacy, and other legal requirements are met. Some organizations choose to have a separate plan for insider threat incident response; these must tie into the general plan.

When the evaluation team reviews the indicators for this capability, it should not differentiate between standalone insider threat incident response plans and general response plans. The same indicators should be used for both situations. The important consideration is that the indicators are met for insider threat events and behaviors.

The basic tenants of response are as follows:

- Responses must be documented and practiced consistently.
- All response procedures should be coordinated with General Counsel.
- Privacy and civil liberties must be considered in response procedures.
- All inquiries should receive a disposition determination after a reasonable period of inactivity.

- All inquiries should have a retrievable record after disposition.
- Until anomalies or allegations are substantiated, the name of the individual must be kept confidential and not revealed outside of those personnel authorized to resolve insider threat concerns.

When insider threat anomalies are detected or when allegations of insider threat behavior are received by the InTP, the organization should conduct an inquiry within the authority of the InTP to either substantiate or refute the information. Well-defined procedures should be established for when and how to open and close an inquiry.

Clearly defined processes for communicating insider threat events and incidents are important to ensure that all affected parties are made aware of the situation. Law enforcement, if involved, should share information when it is available and when law enforcement sensitivity is not essential. These processes should maintain the confidentiality of reporting employees at all times.

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 is suspected insider threat activity investigated and resolved?
- Who is involved in this process?
- How is an inquiry conducted?
- Do insider threat events have a separate response plan or are they covered under existing response plans?
- If insider threat events have a separate process, how does it relate to the general incident response plan?
- Who is responsible for collecting forensic evidence if needed?
- What is the process followed for collecting evidence?
- How are identified malicious insider activities communicated throughout the organization?
- Who is notified if there is an escalation or emergency situation related to mitigating insider threats?
- How is information shared about potential insider threat activity throughout the organization?

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

☐ The InTP has a documented insider threat incident response plan that addresses

Doc Rev

Dir Obs

Intvw

- ☐ how incidents are detected and reported

  Doc Rev

  Dir Obs

  Intvw

- ☐ how incidents are contained, mitigated, remediated, and closed

  Doc Rev

  Dir Obs

  Intvw

- ☐ how incidents are escalated and communicated

  Doc Rev

  Dir Obs

  Intvw

- ☐ how incidents are referred to law enforcement and (if applicable) prosecuted

  Doc Rev

  Dir Obs

  Intvw

☐ roles and responsibilities of InTP team members and others who will be performing any of the investigation, response, and mitigation activities

Doc Rev _____

Dir Obs _____

Intvw _____

☐ points-of-contact for coordination, notification, escalation, and technical support

Doc Rev _____

Dir Obs _____

Intvw _____

☐ how to coordinate responses with legal (for federal agencies, this would be General Counsel), HR, and privacy officers to ensure that privacy and civil liberties are considered

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The incident response plan includes guidelines and procedures that define how insider threat incidents and their related responses are documented.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The incident response plan includes defined processes and related procedures for conducting inquiries or investigations of insider threat activities. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Organizational definitions for insider threat events, incident categories, and priority/severity levels are established and institutionalized.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The incident response plan specifies defined, approved internal and external response options for potential or actual insider threat events and behavior.

Doc Rev

Dir Obs

Intvw

☐ The incident response plan includes a surge support plan to help resolve and remediate insider threat events.

Doc Rev

Dir Obs

Intvw

☐ There is an established chain-of-command for determining the disposition of insider cases.

Doc Rev

Dir Obs

Intvw

☐ A postmortem investigation is conducted after resolution of high impact or poorly handled insider threat event response activities.

Doc Rev

Dir Obs

Intvw

☐ Lessons learned are collected from the postmortem investigation and incorporated into updates to the incident response plan.

Doc Rev

Dir Obs

Intvw

☐ Defined processes and related procedures are in place for collecting forensic evidence when necessary.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The incident response plan includes specific guidance and scenarios for responding to particular types of incidents.

Doc Rev

Dir Obs

Intvw

☐ The incident response plan is periodically reviewed and updated as needed to reflect changes in program needs, constraints, regulations, etc.

Doc Rev

Dir Obs

Intvw

☐ The incident response plan is periodically tested using mock exercises and scenarios.

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)

1.4 Insider Threat Program Communication Plan

A set of documented and maintained plans exists governing the communication and promotion of the InTP and, where applicable, insider threat events.

Clarification/Intent

The organization should create a plan for announcing and promoting the InTP internally. It should also determine which components of the program are made public and which are known only to the InTP team and senior management. For instance, some organizations choose to keep specific parts of the program confidential to a small group of people, such as which data sources are collected and how data is collected and resolved.

Clearly defined processes for communicating insider threat events and incidents are also important to ensure that all affected parties are made aware of the situation. These processes should maintain the confidentiality of reporting employees at all times.

Evaluation Team Guidance

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 information about the InTP has been communicated to the organization?
- How was this information communicated?
- Are there parts of the InTP that are not publicly communicated to the organizational staff?
- If so, which parts? What information?
- What guidance has been developed and institutionalized for communicating insider threat activity?
- Who is involved in developing this guidance?
- What does the guidance cover?
- Who is notified if there is an escalation or emergency situation related to mitigating insider threats?
- How is information about potential insider threat activity shared throughout the organization?

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 communication plan for sharing information about the insider threat program and potential or actual insider threat events has been established and includes

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ defined notification process

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ defined notification timeframe

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ defined information to be conveyed

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ criteria for when not to notify

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ defined process for escalating communications

Doc Rev _____

Dir Obs _____

Intvw _____

☐ defined process for communicating events and incidents that affect classified and sensitive information

Doc Rev _____

Dir Obs _____

Intvw _____

☐ defined process for obtaining and sharing intelligence information, if applicable

Doc Rev _____

Dir Obs _____

Intvw _____

☐ defined data sharing and communication channels across the organization, including IT, physical security, counterintelligence (if applicable), legal, HR, and the InTP team

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The communication plan specifies how to announce and promote the InTP within the organization and identifies which components and details of the program are made public.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The communication plan undergoes periodic review and is updated as needed to reflect changes in program needs, constraints, regulations, etc.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The communication plan is periodically tested using mock exercises and scenarios.

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)

1.5 ERM Integration

The InTP is integrated with the enterprise and/or security risk management program.

Clarification/Intent

All organizations operate under the shadow of risk. Organizations tend to

- focus on threats from outsiders
- overlook the threat from malicious insiders

Insiders have authorized access to critical systems and data, making this risk more difficult to defend against. To make more informed decisions about risks, senior management must understand the dangers posed by malicious insiders.

A risk assessment will inform the insider threat program about which critical assets are at risk and what protections need to be improved or added.

- Security risk assessments need to look for weaknesses that can be exploited by insider threats. The mitigations of such weaknesses must be integral to the insider threat program. Those who identify insider risks and those who mitigate these risks need to work together.
- Enterprise risk assessments identify the nature of critical assets, specify why they are important to the organization, and pinpoint sources of insider threat.

Insider threats therefore need to be included as a potential type of threat. Risk assessors need to understand the nature of such threats in order to identify them.

If an organization already has an enterprise or security risk management program, the InTP should ensure that appropriate consideration is given to risks from both unintentional and malicious insiders.

If no risk management program exists within the organization, implementing such a program should become a priority.

- Coordination with other parts of the organization and senior management will likely be needed to establish a risk management program.
- The new risk management program can start by focusing on insider threats and then expand to address more typical risks.

Evaluation Team Guidance

Assessments of insider risks should focus on critical assets (refer to Capability 1.6). For each critical asset, identify and manage risks from malicious insiders or unintentional insiders. Insiders can include privileged users, employees, contractors and subcontractors, supply chain partners, other trusted business partners, software developers, and executive management. The criteria for impact, probability and priority will help the InTP team understand the relative criticality of an insider risk. Understanding the organization's tolerance for risk will also help the InTP determine which types of insider threats must be prevented and which types can be detected and managed.

Risk management can be implemented and executed in a variety of locations in an organization; the InTP will need to work with that group.

- stand-alone department
- dedicated risk managers
- security group for security risk assessments
- QA or other independent groups
- external contractor

The evaluation team must identify who is conducting ERP within the organization and find out how insider threats are considered. If this job is done by a contractor, interviews may be required to complete this assessment. If a contractor routinely performs risk management for the organization, additional considerations for insider risk associated with trusted business partners should be taken into account.

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 is the risk management process within the organization?
- How are risks involving insiders incorporated into the risk analysis?
- Who performs this activity?
- What types of risks are included?
- Who is provided the information about the risks from insider threats after an analysis or assessment is completed? How is that information communicated?
- What types of mitigations are performed to protect against identified insider threat risks? How is the risk management process conducted within the organization?

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

☐ An insider threat risk assessment is done on a yearly basis and the results are integrated with broader ERP or security risk program.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Security risk assessments (including consideration of insider threats) of mission critical systems, programs, and other assets are conducted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Insider risks are identified and integrated into the ERP on a continuous basis (at any time).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Risks from insider threats are discussed at senior management risk briefings and meetings.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Insider threats, both unintentional and malicious, are treated as a category of risk.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Impacts of risks from insider threats to the organization's mission critical assets, programs, and personnel are identified and considered when making decisions about how to handle these risks and when planning mitigations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Risk criteria for insider threats (probability, impact, priority, tolerance) have been defined and are integrated with ERP risk criteria.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Insider risks are correlated with other types of risks to mission critical assets, programs, and personnel.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures for insider threat and risk assessments are in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Independent, external assessments of insider threat and risk are conducted.

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)

1.6 Critical Asset Identification

Mission-critical assets are identified and documented.

Clarification/Intent

Critical assets include anything that is considered essential or critical to achieving the organization's missions, such as services, business processes, information, people, technology, and facilities. Insider risk assessments should focus on critical assets. All critical assets must be identified and a list of these assets must be kept up to date. An organization may have a considerable number of assets. Determining which assets are mission critical allows the organization to focus their insider threat program resources where they are most needed.

Evaluation Team Guidance

The InTP team needs to know if any compromised assets are critical in order to appropriately respond. Because an organization must prioritize how its budget is allocated for protecting key assets, it will need to identify its most important critical assets.

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 are the critical assets, programs, and personnel that the organization requires to meet its mission?
- How are these critical assets identified?
- How is the list of critical assets, programs, and personnel maintained? Who maintains this list?

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

☐ Criteria for defining what is considered to be mission-critical are in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A documented list of mission-critical software, systems, and information assets is in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The list of mission-critical software, systems, and information assets is updated on a yearly basis.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The list of mission-critical software, systems, and information includes the contact information for the responsible party or supervisor.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ A documented list of mission-critical personnel and other non-information assets is in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The list of all mission critical personnel and other non-information assets is updated on a yearly basis.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The list of mission critical personnel and non-information assets includes the contact information for the responsible party or supervisor.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A defined process specifies how to establish and maintain the list of mission critical assets.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ A review of new assets determines whether they are mission critical and adds them to the list.

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)

2.1 InTP Governance

Adequate program governance and oversight ensures compliance with standards, regulations, and laws.

Clarification/Intent

The InTP requires adequate governance of the InTP program, including sufficient oversight to ensure compliance with applicable standards, regulations, and laws. Oversight could be provided by a steering committee or working council. Compliance evaluations may be provided by internal or external groups.

Team Guidance

Each organization should work in conjunction with Legal Counsel and Privacy Officers to build an InTP. Members of organizational management, the InTP, and steering committee or working council (or an equivalent group) must be familiar with existing legal mandates, statutes, and directives related to InTP implementation as well as privacy and civil liberties law. This familiarity helps to ensure that the program meets all legal requirements and actions, such as those related to user monitoring, confidential reporting, and protecting employee rights. Legal documents that provide a background for an InTP should be reviewed by appropriate organizational personnel. Relevant laws include the Bill of Rights, the Privacy Act of 1974, the Electronic Communications Privacy Act, the Rehabilitation Act of 1973, Title VII of the Civil Rights Act of 1964, civil liberties principles, whistleblower laws, breach reporting laws, minimum standards such as NISPOM or NITTF, and prohibited personnel practices. Compliance evaluations check for the extent of compliance with all applicable laws, regulations, and standards and identify any compliance gaps in the findings. Evaluations can be provided by an internal or external group, but results should always be reported to senior management. Reports to senior management and other stakeholders should include findings on compliance, as well as any relevant challenges, lessons learned, and improvements in compliance since the last report. The steering committee or working council will also provide general oversight and governance for the InTP, ensuring they function as intended and meet their mission.

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:

- Is there a steering committee, working council or some other group of senior managers who provide oversight on the InTP? How do they function?
- How is legal and regulatory compliance with Federal, sector, state, local or organizational mandates within the InTP evaluated?
- How are compliance improvements made to the InTP?
- How would you know if a new law or regulation would impact the operation of your InTP?

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

☐ There is a designated group of senior managers who function as a working council or steering committee to provide general oversight of the InTP.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A defined policy for InTP governance and oversight establishes the authority and process for conducting compliance evaluations, and reporting to senior management or the working council.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Periodic compliance evaluations occur at least annually or on a schedule consistent with audits of other significant program events.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Results of compliance evaluations are reported to senior management (including the working council if one exists) and other stakeholders.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP complies with all relevant laws.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP complies with relevant laws, regulations, and organizational policies protecting classified and sensitive information.

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] Agencies perform self-assessments of compliance with NITTF and NISPOM insider threat policies and standards. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] Results of self-assessments are reported to the federal Senior Information Sharing and Safeguarding Steering Committee [NITTF] [NISPOM].

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] Agencies enable independent assessments, in accordance with Section 2.1(d) of Executive Order 13587, by providing information and access to personnel of the NITTF. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

Level 3

☐ The working council or steering committee has a formal charter, roles, and responsibilities.

Doc Rev

Dir Obs

Intvw

☐ Senior management oversight reviews of InTP compliance follow a defined process.

Doc Rev

Dir Obs

Intvw

☐ Internal compliance evaluations follow a defined process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ External or independent compliance evaluations (if appropriate) follow a defined process.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Improvements identified as the findings of compliance evaluations are implemented.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ If applicable, the InTP complies with standards, regulations, and laws regarding intelligence information.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Compliance evaluations follow documented procedures.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Improvement plans based on compliance evaluation findings are formally documented and tracked.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The working council or steering committee approves and monitors all improvements based on evaluations.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Groups from across the organization (e.g., legal, HR, business lines) participate in and oversee InTP compliance evaluations.

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 Quality, Effectiveness, and Performance of the InTP

The InTP is evaluated for quality, effectiveness, and performance.

Clarification/Intent

The organization requires adequate oversight of the InTP's quality, effectiveness, and performance.

Evaluation Team Guidance

The organization should develop a quality control group that monitors the actions of the InTP to ensure InTP activities meet performance and quality goals, are effective (achieve the desired result), and processes are being appropriately followed. These activities could be performed by an auditing or a quality assurance group. Such a program must ensure the integrity of the InTP and its activities. Reports to senior managers and other stakeholders should include findings of effectiveness, performance, challenges, accomplishments, lessons learned, and improvements since the last report. Quality reviews can also include a method of ensuring those participating in the Insider Threat Program are executing their responsibilities appropriately (this is often referred to as "watching the watchers". This is particularly important regarding staff who are reviewing indicators and data sources or handling inquiries and investigations.

Note that the compliance evaluations in Capability 2.1 have a different focus, on meeting laws and regulations, while this capability focuses on quality of products and processes, effectiveness of processes, and performance of activities. It is looking to ensure that the InTP is meeting its mission and doing so in a quality manner, meeting the parent organization's general policies and procedures, including HR, performance monitoring, etc.

Compliance versus quality evaluations may be performed by the same group (external third party, internal audit, internal quality assurance, performance management) or may be performed by different groups. For example, in the case where different groups perform the difference types of audits, an external audit team could be responsible for evaluating compliance while an internal QA team evaluates quality and performance. It is also possible to cover all these aspects (both compliance and quality/performance) with one evaluation process performed by the same auditing team. In this case there will be overlap between capabilities 2.1 InTP Governance and 2.2 Quality, Effectiveness, and Performance.

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 is the process for evaluating quality, effectiveness, and performance of the Insider Threat Program?
- Who performs this type of evaluation process?
- How are findings reported and to whom?
- How are improvements made to the Insider Threat Program?
- Are there designated individuals or processes for ensuring that members of the InTP execute their responsibilities in an appropriate fashion (i.e. watching the watchers?)

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 defined policy for quality, effectiveness, and performance is in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ InTP team members have defined roles and responsibilities that can be used as a basis for evaluating their performance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Defined processes for performing InTP activities are enforced.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Periodic evaluations of quality, effectiveness, and performance are conducted at least annually or on a schedule consistent with audits of other significant program events.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Evaluation results are reported to senior management and other stakeholders, such as the working council or steering committee if there is one.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Adherence to organizational policies and procedures is routinely audited and corrections made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Defined processes for internal (self-assessment) of quality, effectiveness, and performance are in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Quality, effectiveness, and performance improvements that are identified as a result of evaluations are implemented.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ External, or independent, reviews of quality, effectiveness, and performance are conducted.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures for QA and effectiveness reviews are in place.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The effectiveness and performance of key InTP activities are evaluated using defined metrics.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The QA reviews ensure the InTP personnel are appropriately executing their responsibilities.

Doc Rev

Dir Obs

Intvw

☐ Lessons learned related to the functioning of the InTP are collected.

Doc Rev

Dir Obs

Intvw

☐ Improvement plans based on the findings of all evaluations, compliance and quality reviews are formally documented and tracked.

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)