Carnegie Mellon University
Software Engineering Institute

Insider Threat Program Evaluation (ITPE)

Capability Questions and Indicators Workbook: Data Collection and Analysis

https://www.sei.cmu.edu

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.

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 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.

This workbook, Data Collection and Analysis, measures the integrated data analytic capability of an organization's InTP. It focuses on the process for identifying and acquiring data sources and their correlation and review for anomalies or suspicious behaviors. It also covers the organization's capability for user activity monitoring. The ITPE workbook for Human Resources and

® 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

Legal includes policies and procedures that support some of these infrastructure activities. The workbook also includes the capability for handling insider incidents through the execution of response actions. The ITPE workbook for Program Management also includes capabilities that support response activities, such as having an incident response plan.

This workbook has one more additional Scoring Level within each capability. A Blue shaded level named "Other". This area is to capture any processes, tools, or data sources that the organization uses to meet the capabilities that are not covered by the current indicators. Having this area can also provide ideas for future indicators, if any "other" processes, tools, or practices are uncovered. Note, that these blue other areas may not be used for all evaluations. In fact they probably will not be, but are put in to provide an area to capture information if needed. The blue level is NOT seen as a more robust level than a Level 4. It's just a way to capture what they are doing, if it helps them meet the capability. There is not score for the blue level and it does not get added to the existing levels, information captured in it can be used in writing the report as a way to show any good actions the organization is performing that were not called out by the evaluation.

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 Executing Response

The organization responds to and mitigates identified potential or ongoing insider threats and activities.

Clarification/Intent

An InTP requires a well thought-out, documented, and practiced response process 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 process should include identified channels for communication, coordination, and hand-off to other organizational units for mitigation (where appropriate).

Team Guidance

The established response capability can be executed using a specialized response process and personnel that are developed as part of the InTP. Alternatively, it can be executed using existing organizational units such as counterintelligence, forensics, personnel security, security operations center (SOC), and computer security incident response teams (CSIRTs).

Collecting forensic evidence and analyzing digital media can be done in-house or externally.

Internal entities that may have authority for conducting inquiries or investigations include (but are not limited to) security offices, personnel security or in the federal government the Office of Inspector General. External investigative entities may include the FBI, DoJ, or military investigative services. Referrals should be based on organizational (or where appropriate federal) policies or statutory requirements. Section 811 of the Intelligence Authorization Act for FY 1995 contains investigative referral requirements for federal agencies.

Capability 1.3, Insider Threat Response Plan, within the ITPE Program Management Workbook, is related to this capability (1.1, Executing Response). The Program Management capability focuses on establishing an Insider Threat Response Plan. This Data Collection and Analysis capability focuses on the execution of that plan. Open-ended questions for both capabilities (below) are very similar.

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?
- What is the response to alerts that identify anomalous insider behavior?
- 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 process is followed to collect and validate 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 organization has an established capability to respond to and mitigate identified potential or ongoing insider threats and activities. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Identified insider threat behaviors and activities are mitigated and resolved. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization follows established procedures or guidelines for responding to and mitigating insider threats, including but not limited to: [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ validation of collected alerts and reports [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ inquiries or investigations to clarify or resolve insider threat matters [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ documenting each reported insider threat behavior or activity [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ documenting each confirmed insider threat activity [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ handing off investigations, inquiries, and mitigations to appropriate internal or external entities [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ coordinating and communicating insider threat mitigation and response tasks across the organization to contain and resolve the activity, including (but not limited to) IT, HR, physical and personnel security, counterintelligence, InTP staff, and data owners [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Resolution of insider threat matters occurs in a timely fashion, as defined by organizational or federal criteria. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ All response and mitigation actions are conducted in accordance with applicable laws, whistleblower protections, civil liberties, and privacy policies. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government Only] Response actions are centrally managed by the InTP within the agency or one of its subordinate entities. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government Only] Investigations or inquiries are referred as required (based on organizational or federal policy) to internal or external entities with the appropriate authority to conduct them. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

Level 3

☐ Additional staff are identified and called in if needed to assist with resolving and remediating insider threat events.

Doc Rev

Dir Obs

Intvw

☐ The established chain-of-command is followed to effect a disposition of all insider threat cases.

Doc Rev

Dir Obs

Intvw

☐ Forensic evidence is collected if necessary.

Doc Rev

Dir Obs

Intvw

☐ Digital media is analyzed if necessary.

Doc Rev

Dir Obs

Intvw

☐ Forensic evidence collection and digital media analysis follow best practices, including (but not limited to) chain of custody rules.

Doc Rev

Dir Obs

Intvw

Level 4

☐ Documented procedures specify the process and mechanisms to reconstitute and recover critical systems that are affected by insider threat events.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Appropriate IT, HR, physical and personnel security, counterintelligence, InTP staff, and data owners are trained on procedures, processes, and mechanisms for responding to and resolving insider threat events.

Doc Rev _____

Dir Obs _____

Intvw _____

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

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Improvements to the incident response process are made based on lessons learned.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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 Information Access Management

Processes exist to minimize barriers to InTP access to relevant information in an efficient and secure manner.

Clarification/Intent

To identify, analyze, and resolve insider threat allegations and threats, InTP staff must have access to data from other parts of the organization. This data must be provided in a secure and timely manner either manually or electronically. The InTP staff may be given the data directly or granted authorized access to it.

InTP staff should use established, institutionalized methods and procedures for requesting necessary information. Alternatively, the other components of the organization may regularly report such information to the InTP staff.

Team Guidance

Sensitive or protected information includes but is not limited to information held by "special access, law enforcement, inspector general, or other investigative sources or programs,"[4] which may require senior or executive management approval for access. Note that capabilities 2.2, 2.3, and 2.4 deal with some specific types of information needed by the 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:

- How is this data passed from organizational components to the InTP staff or the InTP analytic capability?
- Who is involved in the exchange?
- In what timeframe is data passed?
- How does the InTP staff request access to data that it does not receive on a regular basis?
- What authority and approval does the InTP staff have to receive this data?
- What directives from management have been given to organizational components to provide information to the InTP?

Agency Response

Evidence Sought

Auto Verification

[4] Source: NITTF Minimum Standards available at: http://fas.org/sgp/obama/insider.pdf

Additional Information

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ Senior or executive management has directed components of the organization to provide data sources and other information to the InTP staff that are necessary to identify, analyze, and resolve insider threat matters. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Data sources and other relevant information are provided in a secure manner. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Data sources and other relevant information are provided in a timely manner, according to organizational requirements. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Procedures are established for the InTP staff to request access to organizational components involving sensitive or protected information. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The organization has guidelines for counterintelligence, physical and personnel security, IT, HR, and other relevant components to report information about insider threats directly to the InTP staff. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ The InTP staff has timely access to analytic products pertaining to adversarial threats, based on organizational requirements. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

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

Doc Rev

Dir Obs

Intvw

Level 3

☐ New data sources are reviewed for applicability to the InTP.

Doc Rev

Dir Obs

Intvw

☐ Documented policies and procedures specify the processes and mechanisms used by the InTP to gain access to new data sources, including but not limited to

Doc Rev

Dir Obs

Intvw

- ☐ justifying the need for new or additional data access

  Doc Rev

  Dir Obs

  Intvw

☐ obtaining sign-off from legal and management

Doc Rev

Dir Obs

Intvw

☐ specifying in-motion and at-rest security requirements for the new data to be collected

Doc Rev

Dir Obs

Intvw

☐ resolving technical issues with data source providers

Doc Rev

Dir Obs

Intvw

Level 4

☐ Processes, procedures, and mechanisms for providing information to the InTP are reviewed on a regular basis to identify improvements.

Doc Rev

Dir Obs

Intvw

☐ Organizational components and InTP staff receive training on procedures, processes, and mechanisms for the InTP staff to request information for detecting, analyzing and resolving insider threat matters.

Doc Rev

Dir Obs

Intvw

☐ Organizational components and InTP staff receive training on procedures, processes, and mechanisms to provide information for detecting analyzing, and resolving insider threat matters.

Doc Rev

Dir Obs

Intvw

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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 Access to Technical Information

Relevant organizational components securely provide InTP staff with the technical information necessary to identify, analyze, and resolve insider threat activities.

Clarification/Intent

To identify, analyze, and resolve insider threat allegations and threats, InTP staff must have access to data from other parts of the organization. This data must be provided in a secure and timely manner either manually or electronically. The InTP staff may be given the data directly or granted authorized access to it. Technical information includes but is not limited to information assurance data. InTP staff should use established, institutionalized methods and procedures for requesting necessary information (as defined in Capability 2.1). Alternatively, the other components of the organization may regularly report such information to the InTP staff.

Team Guidance

Sensitive or protected information includes but is not limited to information held by "special access, law enforcement, inspector general, or other investigative sources or programs,"[5] which may require senior or executive management approval for access.

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 technical data is passed from organizational components to the InTP staff or the InTP analytic capability?
- Who is involved in the exchange?
- What authority and approval does the InTP staff have to receive this date or the organizational unit's staff have to send the data?

Agency Response

Evidence Sought

Auto Verification

Additional Information

[5] Source: NITTF Minimum Standards available at: http://fas.org/sgp/obama/insider.pdf

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The technical data that must be sent to the InTP or for which access is to be allowed is defined in policy or guidance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Technical data reported to the InTP or for which access is allowed includes but is not limited to [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ personnel usernames and aliases [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ levels of network access [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ audit data [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ unauthorized use of removable media [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ print logs [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Technical data reported to the InTP or for which access is allowed includes incident reports.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The effectiveness of sharing technical information is evaluated periodically and improvements are made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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)

2.3 InTP Access to HR Information

HR securely provides InTP staff with the information necessary to identify, analyze, and resolve insider threat activities.

Clarification/Intent

To identify, analyze, and resolve insider threat allegations and threats, InTP staff must have access to data from HR. This data must be provided in a secure and timely manner either manually or electronically. The InTP staff may be given the data directly or granted authorized access to it.

HR data can include personnel files, payroll information, disciplinary actions, time and attendance records, and where appropriate, performance reviews.

InTP staff should use established, institutionalized methods and procedures for requesting necessary information. Alternatively, the other components of the organization may regularly report such information to the InTP staff.

Team Guidance

Sensitive or protected information includes but is not limited to information held by "special access, law enforcement, inspector general, or other investigative sources or programs,"[6] which may require senior or executive management approval for access.

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 HR-related data is passed from organizational components to the InTP staff or the InTP analytic capability?
- Who is involved in the exchange?
- What authority and approval does the InTP staff have to receive this date or does HR staff have to send the data?

Agency Response

Evidence Sought

Auto Verification

Additional Information

[6] Source: NITTF Minimum Standards available at: http://fas.org/sgp/obama/insider.pdf

Scoring Criteria

Level 1

Fails to meet the requirements of the higher levels.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 2

☐ The HR data that must be sent to the InTP or for which access is to be allowed is defined in policy or guidance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ HR data sources comprise all relevant HR databases and files, including but not limited to [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ personnel files [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ payroll and voucher files [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ outside work and activities requests [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ disciplinary files [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ personnel contact records (as may be necessary for resolving or clarifying insider threat matters) [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ HR data sources also include

Doc Rev _____

Dir Obs _____

Intvw _____

☐ performance reviews, where appropriate

Doc Rev _____

Dir Obs _____

Intvw _____

☐ time records

Doc Rev _____

Dir Obs _____

Intvw _____

☐ HR alerts

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The effectiveness of sharing HR information is evaluated periodically and improvements are made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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)

2.4 InTP Access to Counterintelligence and Security Information

Relevant organizational components securely provide InTP staff with the counterintelligence and security information necessary to identify, analyze, and resolve insider threat activities.

Clarification/Intent

To identify, analyze, and resolve insider threat allegations and threats, InTP staff must have access to counterintelligence and security data from other parts of the organization. This information may come from a security office, counterintelligence group or some other part of the organization. The sources of this information will need to be identified and agreements made to receive or access the necessary data. This data must be provided in a secure and timely manner either manually or electronically. The InTP staff may be given the data directly or granted authorized access to it.

Access and information includes but is not limited to

- counterintelligence and security data
- physical security data
- financial data
- other behavioral data

InTP staff should use established, institutionalized methods and procedures for requesting necessary information. Alternatively, the other components of the organization may regularly report such information to the InTP staff.

InTP staff with a need-to-know should also have access to available intelligence reports and analytic products pertaining to adversarial threats as appropriate to organizational sector and policy.

Team Guidance

Sensitive or protected information includes but is not limited to information held by "special access, law enforcement, inspector general, or other investigative sources or programs,"[7] which may require senior or executive management approval.

Some organizations do not have counterintelligence groups or data. When assessing such organizations, only focus on security data. If they do not have counterintelligence data – it should not count against them, if it is not applicable to their organization and sector.

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 counterintelligence and security data is passed from organizational components to the InTP staff or the InTP analytic capability?
- Who is involved in the exchange?
- What authority and approval does the InTP staff have to receive this date or does HR staff have to send the data?

Agency Response

Evidence Sought

[7] Source: NITTF Minimum Standards available at: http://fas.org/sgp/obama/insider.pdf

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 counterintelligence and security data that must be sent to the InTP or for which access is to be allowed is defined in policy or guidance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The counterintelligence and security data sources include but are not limited to [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

- ☐ personnel security files [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ polygraph examination reports, where appropriate [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ facility access records [NITTF] [NISPOM]

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ security violation files [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ travel records [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ foreign contact reports [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ financial disclosure filings [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ confidential reports of suspicious behaviors or potential insider activity [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ [For U.S. Federal Government Only] The InTP staff has timely access to U.S. government intelligence and counterintelligence information pertaining to adversarial threats, based on organizational requirements. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ Counterintelligence and security data sources also include background check or security clearance information.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ The effectiveness of sharing counterintelligence and security information is evaluated periodically and improvements are made as needed.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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)

2.5 User Activity Monitoring

The organization monitors user activity on its networks and systems.

Clarification/Intent

The organization established and maintains a program to monitor, log, and audit the activities of employees and other users on its networks and systems, based on its defined requirements and in keeping with any legal or privacy rules.

User Activity Monitoring (UAM) is performed for both unclassified and classified systems. Monitoring of classified user activity is only applicable to organizations with classified systems and networks.

Team Guidance

The organization has established its right to monitor, log, and audit both the technical and interpersonal conduct of employees and other users on its digital media, networks, and other computerized communication media. "Other users" include trusted business partners and any visitors that may come to the systems as part of line of business operations.

The organization does not have to specify what is being monitored or how it is being monitored. Monitoring can be done internally or via agreement with external organizations.

The ITPE HR and Legal workbook includes a corresponding capability (3.1 User Monitoring Policy). The User Monitoring Policy capability questions also apply to user activity monitoring.

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:

- Has a formal user activity monitoring program been established within the organization?
- What does this program entail?
- What types of data and activities are collected?
- Who is responsible for employee or user monitoring?
- How is the data protected?
- If the organization has classified networks or systems, how are they monitored?

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 includes the technical capability to monitor user activity on all organizational networks and systems. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The InTP staff analyzes the following data for concerning behavior:

- ☐ email logs

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ chat logs

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ phone logs

  Doc Rev _____

  Dir Obs _____

  Intvw _____

- ☐ web browsing activity

  Doc Rev _____

  Dir Obs _____

  Intvw _____

☐ All user monitoring activity is conducted in accordance with applicable laws, whistle-blower protections, civil liberties and privacy policies. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] The InTP includes the technical capability to monitor user activity on all organizational classified networks and systems. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] As required by the organization, service level agreements (SLAs) are executed with all other agencies or organizations that operate or provide classified network connectivity or systems. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

☐ [For U.S. Federal Government Only] If UAM is outsourced, there is an SLA with the provider that details the methods employed to identify suspicious user behavior and how that information shall be reported to the subscriber's insider threat personnel. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

Level 3

☐ The organization monitors social media related to its employees and its brand.

Doc Rev

Dir Obs

Intvw

☐ The InTP team has access to decrypted HTTPS traffic.

Doc Rev

Dir Obs

Intvw

☐ The InTP team has access to mobile device logs on organization-owned devices.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ New data sources are reviewed to determine whether user activity must be monitored.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Processes, procedures, and mechanisms for performing user activity monitoring are reviewed on a regular basis to identify improvements.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Documented procedures specify the process and mechanisms to perform user activity monitoring.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Organizational components and InTP staff receive training on procedures, processes, and mechanisms related to operating and maintaining the user activity monitoring program.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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)

2.6 Integrated Data Analytical Capability

The organization has established and maintains an insider threat analytic capability to gather, review, and assess information.

Clarification/Intent

One of the main components of an InTP is the ability to fuse together data from multiple sources to detect potential or ongoing insider threat behaviors and actions. Data comes from various sources (listed in Capability 2.1 InTP Access to Information) which include but are not limited to information derived from IT, HR, Legal, user activity monitoring, counterintelligence, personnel and physical security and other sources. The analytical capability is able to aggregate technical and behavioral data from disparate sources. Such analysis

- identifies anomalies and resolves allegations of insider threat activity
- produces a better "whole person" picture and provides context to insider threat anomalies and allegations
- performs focused observations

Data should only be accessible by the InTP team members who are conducting the analysis. Whenever possible,

- Analyzers should not be data collectors
- Data collectors should not be analyzers

Data that is analyzed and produces an allegation or supports an inquiry/investigation should meet the standards for "best evidence."

Team Guidance

Analytic capability may take the form of a formalized, automated data analysis hub or a smaller, focused data analysis activity with less automation. Data analysis does not have to be performed with a specific tool; it may employ many tools or even none at all. Tools and techniques may include but are not limited to

- Commercial of the Shelf (COTS) / Government off the Shelf (GOTS) analysis tools for automated analysis
- large data pattern analysis (such as the Statistical Package for the Social Sciences (SPSS), *Non-obvious relationship awareness* (*NORA)*, Mahout[8], or custom code) for customized or targeted analysis
- specific incident exploration
- focused collections

Data can be collected and integrated electronically, manually, or a combination of both. Timeliness of data collection is necessary to avoid working with stale data.

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 are behavioral and technical data correlated?
- What type of alerts are produced that trigger inquiries or investigations?
- Who performs insider threat analysis?

Agency Response

Evidence Sought

[8] Mahout is software from APACHE used for scalable machine learning and data mining.

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 established a defined analytical capability. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Processes are in place to maintain the analytical capability and keep it current. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Analysts have been identified and trained to perform the required analytical activities. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ The analytical capability allows for the integration, review, and assessment of information from organizationally defined sources. [NITTF] [NISPOM]

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Insider threat data is aggregated with tools to make manual and automated analysis feasible and scalable (SIEM, custom tools, etc.).

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Logs are maintained for a sufficient period.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 3

☐ The InTP includes defined criteria for handling alerts and escalation of potential events.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Controls are in place to ensure log integrity.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Data collection occurs within an acceptable timeframe based on risk acceptance.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Tools used to perform data correlation and analysis are restricted for access by only members of the InTP Team or those approved by the InTP Program Manager.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Outputs and findings from the analysis are protected and secured.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Outputs and findings from the analysis are provided only to those with an approved reason to know.

Doc Rev _____

Dir Obs _____

Intvw _____

Level 4

☐ Documented procedures specify the process and mechanisms to perform insider threat analysis.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Relevant organizational components and InTP staff receive training on procedures, processes, and mechanisms related to the operation and maintenance of the analytical capability.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Documented procedures specify the process and mechanisms used to evaluate the effectiveness of the established analytical capability and plan the implementation of selected improvements.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ A continuity of operations plan for continuing operation of the analytical capability during crisis events or outages has been developed, implemented, and tested.

Doc Rev _____

Dir Obs _____

Intvw _____

☐ Surge support or backup staff are in place to help perform analytics during crisis events or after business hours if necessary.

Doc Rev _____

Dir Obs _____

Intvw _____

Other

☐ _____

_____

_____

Doc Rev _____

Dir Obs _____

Intvw _____

☐ _____

_____

_____

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)