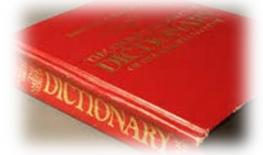




DEFINITIONS AND REFERENCES



Definitions:

Insider. Cleared contractor personnel with authorized access to any Government or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

Insider Threat. The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

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

Requirements:

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

References:

- DoD 5220.22-M Change 2 (NISPOM)
- DSS Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM Version 3.3 Apr 2016

[Templates Available Here](#) Customizable templates for Insider Threat Implementation Plan.



Establishing an Insider Threat Program (ITP) Best Practices:

Phases

Evaluation Phase:

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

Formulation Phase:

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

Implementation Phase:

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



Establishing an Insider Threat Program Best Practice: Core Elements

1. **Operations Management & Planning:** refers to the implementation plan, leadership, policy creation, legal and privacy review, plan development, implementation, and administration of the core program elements. This element includes support of the ITP program by senior leadership at the facility.
2. **Gather:** refers to the processes of gathering information and evaluating it to determine the appropriate reporting channels. In this process you will create and maintain an inventory of behavioral indicators associated with Insider Threats. You will also define metrics to evaluate performance. This process helps to reduce false positives and improves identification rates. It also provides guidance for monitoring strategies and informs senior leadership.
3. **Collaboration:** refers to the use of internal and external relationships to facilitate the acquisition, sharing and reporting of information potentially indicative of Insider Threat behaviors and activities.
4. **Education:** refers to the processes associated with Insider Threat education, training, and awareness programs apportioned appropriately with the basic, intermediate, and advanced program models.
5. **Protection Specification:** refers to risk assessment processes aimed to identify assets, competitive and threat landscape, vulnerability analysis, legal liability, security implications to business viability, profitability, reputation, and personal safety.
6. **Counterintelligence:** refers to a programmatic approach to the identification, disruption, neutralization, and mitigation of Insider Threats.
7. **Monitoring:** refers to the designation and implementation of manual or automated technical monitoring technologies, processes, and protocols essential for the accomplishment of the program objectives delineated in the respective model: basic, intermediate, or advanced.
8. **Incident Response:** refers to the procedures and protocols to respond to technical and non-technical indicators, incidents, and events. Procedures will be implemented to direct and indirect interventions, investigations, and other similar follow-up.
9. **Audit & Improvement:** refers to review and audit management processes required to assure that the program is operating pursuant to plan, identifies lessons learned, and implements improvements based on metrics and other analysis.



Monitoring Classified Network Activity Getting Started: Key Elements

- **Monitoring Considerations:** Once you determine what you are going to monitor, you must determine how you are going to monitor the activities. Questions to ask include:
 - How will data be integrated?
 - How will data be analyzed?
 - How will results be reported?
- **Integration:** In order to detect potential Insider Threats, your program needs to integrate the data it collects so it may be viewed as a whole. There are two common methods for integrating data – they are known as “push” and “pull.” Many programs use a combination of these two methods. Using the push method, collected data is pushed to the appropriate Insider Threat program personnel automatically. This streamlines the collection process and helps ensure the timely analysis of data. However, if too many requirements are programmed into the system, it may swamp the system with data. With the pull method, an analyst retrieves data from several locations. This allows the analyst to request smaller and more specific queries. However, the timeliness and consistency of collection depends on the analyst’s workflow. When determining how your program will integrate data, you will need to take into account your organization’s resources, staffing, and network setup.
- **Audit Requirements:** Auditing and monitoring requirements apply to all auditable devices on the accredited system. Operating systems, firewalls, routers, intrusion detection devices, etc. should be monitored and reviewed for anomalies through the use of audit trails. Contractors’ auditing and monitoring policies and procedures will include efforts to detect activity indicative of Insider Threat behavior, along with procedures for reporting such activity to the FSO and ITSO. The policies and procedures will include how to properly protect, interpret, store data, and limit access to user activity monitoring methods and results to authorized personnel.

Audit records will include the following:

Enough information to determine the action involved, the date and time of the action, the system on which the action occurred, the system entity that initiated or completed the action, and the resources involved (if applicable);

Successful and unsuccessful logins and logoffs;

Unsuccessful accesses to security-relevant objects and directories;

Changes to user authenticators;

The blocking or blacklisting of a user ID, terminal, or access port

Denial of access from an excessive number of unsuccessful login attempts



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

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

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

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

Guidelines for reviewing automated audit records:

- Review and verify there have been no changes to system time and that the automated audit functions are performing properly. Review BIOS changes and other configuration changes not identified in the SSP.
- Review all failed logins. Question multiple failed login attempts and account lockouts
- Review a sampling of successful logins to ensure those persons were actually present and using their account during the recorded time periods. For example, if you are aware of someone being on travel or on vacation during the week, verify his or her account was not accessed.
- Question login sessions that occur at unusual times (e.g., 2:00 a.m.) or sessions that are left open for long periods of time.
- Scrutinize direct logins to generic or group accounts. Verify they are within the guidelines specified in the (M)SSP.
- If applicable, verify accesses to privileged group/generic accounts were made from authorized user IDs.
- Depending on the available audit mechanism, failed attempts to access objects may be all inclusive rather than limited to security-relevant objects. Attempt to focus your review on identifying any user ID that consistently has failed access attempts to privileged system files.



Gather:

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

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

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

Reporting:

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