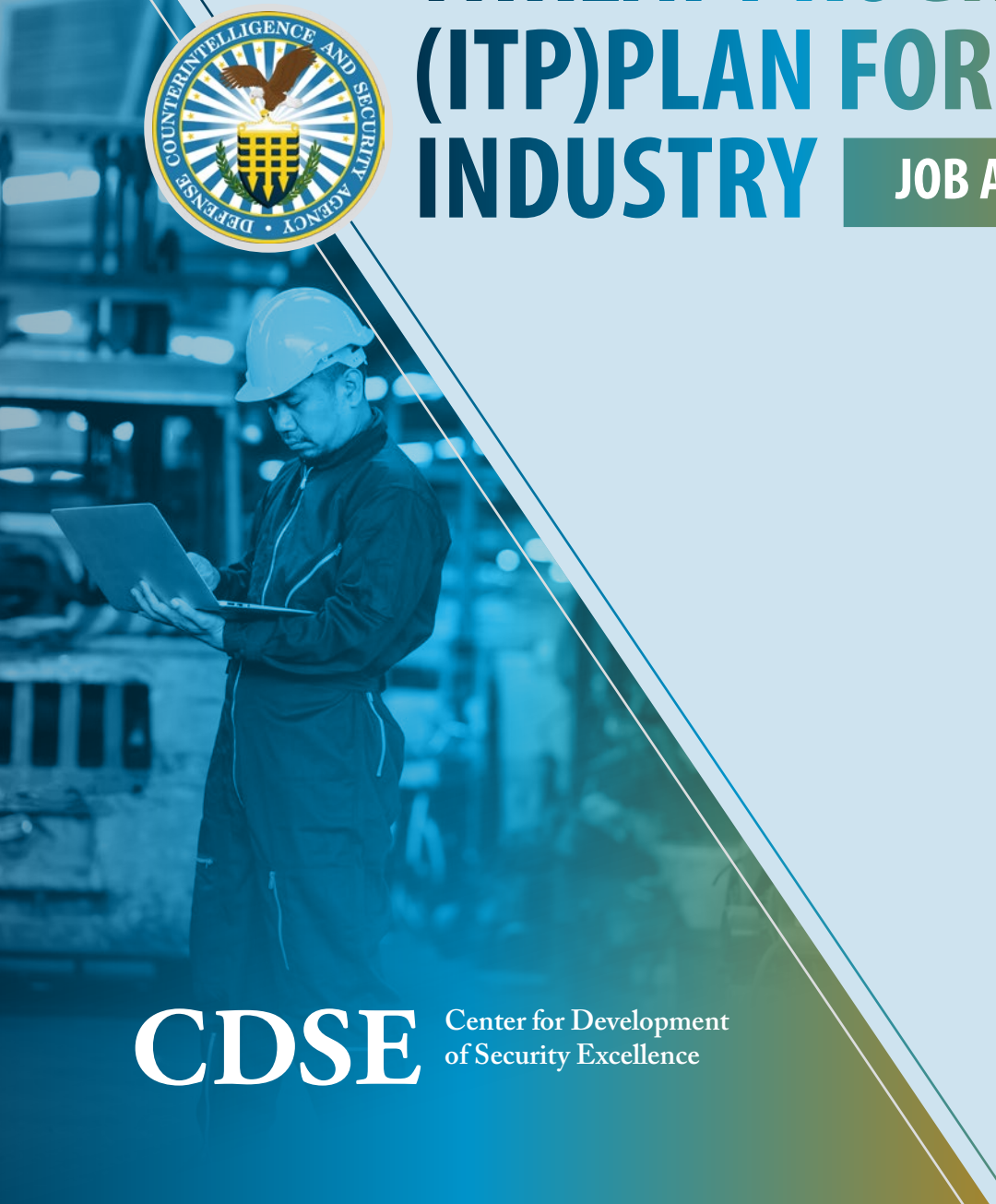
DEC. 2022

SAMPLE INSIDER THREAT PROGRAM (ITP)PLAN FOR INDUSTRY

JOB AID



CDSE Center for Development of Security Excellence

This information within this job aid is intended for use as a sample. It is not a template. An organization's plan must be tailored to the specific Insider Threat Program (ITP) procedures and processes in place at the organization.

OVERVIEW

I. Purpose.

This plan establishes policy and assigns responsibilities for the Insider Threat Program (ITP). The ITP will establish a secure operating environment for personnel, facilities, information, equipment, networks, or systems from insider threats. 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 threats may also include any actions that result in damage caused by fraud, sabotage, trade secret theft, espionage, resource degradation, and workplace violence.

The program will gather, integrate, and report relevant and credible insider threat-related information covered by the National Security Adjudicative Guidelines. These guidelines, issued in the Security Executive Agency Directive 4, hold employees granted personnel clearances (PCLs) and employees awaiting PCLs to a higher standard. It functions partially as an insider threat deterrence mechanism.

The program detects risks to classified information from insiders, and addresses the risk of violence or other degradation by an insider affecting government or contractor resources, including personnel, facilities, information, equipment, networks, or systems.

II. Scope and applicability.

[Name of Organization] is subject to insider threats and will take actions to address threats and personnel at risk of becoming a threat.

[Name of Organization] will continually identify and assess threats to the organization and its personnel and implement a program with capabilities designed to reduce risk.

This Insider Threat Program Plan applies to staff offices, regions, and personnel with access to government or contractor resources including personnel, facilities, information, equipment, networks, or systems.

III. Policy.

The ITP will protect personnel, facilities, and automated systems from insider threats in compliance with 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual (NISPOM), also known as the "NISPOM rule." This program will prevent espionage, violent acts against the Nation, or the unauthorized disclosure of classified information and controlled unclassified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems; and mitigate the risks to the security of classified information through administrative, investigative, or other responses.

The ITP will meet or exceed the minimum standards for such programs, as defined in § 117.7 (d) of the NISPOM rule with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and Defense Counterintelligence and Security Agency (DCSA) Assessment and Authorization Process Manual (DAAPM) under the NISPOM rule.

TERMS AND DEFINITIONS

- **Insider**: cleared personnel with authorized access to any USG 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 ability to meet their obligations to protect classified national security information.

PROGRAM ROLES AND RESPONSIBILITIES

The contacts listed below are considered essential personnel behind the functionality of the insider threat program and its capacity to gather, integrate, analyze, and respond appropriately to pertinent insider threat-related information.

Access Control Officer
Grant access for personnel to facility; observe, and report suspicious or criminal activities, patrol, and/or secure assigned areas.
Name:
Email Address:
Telephone:
Employee Assistance Program Representative
Coordinate access to the voluntary, work-based program that offers free and confidential assessments, short-term counseling, referrals, and follow-up services to employees who have personal and/or work-related problems.
Name:
Email Address:
Telephone:
Human Resources Officer (HRO)
Screen employees and train managers; work with employee relations personnel, possess knowledge about employee assistance programs; and respond to employee matters including work performance, disciplinary actions, or termination.
Name:
Email Address:
Telephone:

Facility Security Officer (FSO)
Supervise and direct security measures necessary for implementing requirements for the security program, and ensure protection of classified information.
Name:
Email Address:
Telephone:
Information System Security Manager (ISSM)
Verify the implementation of the information system security program and ensure continuous monitoring strategies; conduct self-inspections, and verify corrective actions.
Name:
Email Address:
Telephone:
Insider Threat Program Senior Official (ITPSO)
Implement ITP activities, such as, daily operations, management, and ensuring compliance with minimum standards outlined in the NISPOM rule.
Name:
Email Address:
Telephone:
Insider Threat Program Manager
Manage insider threat matters and any hub analysts, ensuring potential future investigational viability and/or operational capability are preserved and privacy and civil liberties of the workforce are respected.
Name:
Email Address:
Telephone:
Legal Advisor
Ensure any legal, privacy, civil rights, and civil liberties issues (including, but not limited to, the use of personally identifiable information) are appropriately addressed.
Attorney Name:
Email Address:
Telephone:

Payroll Officer
Calculate employees' compensation, update internal payroll databases, and ensure timely payments, and government reporting.
Name:
Email Address:
Telephone:
Senior Management Official
Ultimate authority for the facility's operations that directs actions necessary for the safeguarding of classified information in the facility.
Name:
Email Address:
Telephone:

ORGANIZATIONAL CAPABILITY

I. Insider Threat Program Senior Official

(1) The Insider Threat Program Senior Official (ITPSO) will be designated in writing and will act as the company's representative for ITP implementing activities. The designated ITPSO will be cleared in connection with the facility clearance, be a United States citizen, and will be designated as Key Management Personnel (KMP) in the National Industrial Security System (NISS) in accordance with Cognizant Security Agency (CSA) guidance and § 117.7 (b).

(2) The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived from 32 Code of Federal Regulation Part 117, National Industrial Security Program Operating Manual (NISPOM). Responsibilities include:

a. Self-certify the Insider Threat Program Plan in writing to DCSA.

b. Provide copies of the Insider Threat Program Plan upon request and make the plan available to the DCSA Industrial Security Representative (ISR) during the Security Review and Rating Process.

c. Establish an Insider Threat Program based on the organization's size capabilities and complexities.

d. Provide Insider Threat training for Insider Threat Program personnel and awareness training for cleared employees in accordance with § 117.12 (g)(2) of the NISPOM rule.

- **ITP Personnel Training**

(1) All personnel assigned duties related to insider threat program management will attend the training outlined in § 117.12 (g)(1) of the NISPOM rule.

(2) After initial implementation of this plan and completion of the required training, all new contractor personnel assigned duties related to the insider threat program

management will complete the above training within 30-days of being assigned duties and refresher training annually thereafter.

- **Employee Insider Threat Awareness Training**

  (1) Training on insider threat awareness in accordance with § 117.12 (g)(2) of the NISPOM rule will be required for all cleared employees before being granted access to classified information and annually thereafter.

  (2) Cleared employees already in access will complete insider threat awareness training no later than MMM DD YYYY and annually thereafter in accordance with § 117.12 (g)(2).

  (3) All cleared employees who are not currently in access will complete insider threat awareness training prior to being granted access and annually thereafter in accordance with § 117.12 (g)(2) of the NISPOM rule.

- **Insider Threat Program Senior Official (ITPSO) Training**

  (1) ITPSO training will be completed by MMM DD YYYY

  (2) If a new ITPSO is appointed after the 6-month implementation period, the new ITPSO will complete the required training within 30-days of being assigned ITPSO responsibilities.

- **Insider Threat Training Records Management**

  (1) Insider Threat Training Records will consist of training attendance records, certificates, or other documentation verifying that personnel completed the training requirements in accordance with § 117.12 (g)(3).

  (2) Insider Threat Training Records will maintain records of all employee insider threat awareness initial and refresher training in accordance with § 117.12 (g)(2).

  (3) Insider Threat Training Records will be available for review during DCSA Security Review and Rating Process.

  (4) Insider Threat Awareness will be included in annual refresher training to reinforce and update cleared employees on the information provided in initial training in accordance with § 117.12 (g)(2).

e. Establish user activity monitoring on classified information systems in order to detect activity indicative of insider threat behavior. These monitoring activities will be based on Federal requirements and standards (Federal Information Security Management Act, National Institute of Standards and Technology, and Committee for National Security Systems) and in accordance with § 117.18 (a)(2) and (b)(4).

f. Establish procedures in accordance with § 117.7(d) to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 and Presidential Memorandum "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs."

- **Insider Threat Reporting Requirements.**

  (1) All credible Insider Threat information will be coordinated and shared with the ITPSO, which will then take action as directed in §117.8 (a)(1). The following information will be reported:

    a. Information regarding cleared employees, to include information indicative of a potential or actual insider threat and which falls into one of the 13 adjudicative guidelines, which must be reported when that information constitutes adverse information, in accordance with 32 CFR §117.8 (c)(1), ISL 2006-02, and ISL 2011-4.

    b. Incidents that constitute suspicious contacts, in accordance with 32 CFR §117.8 (c)(2) and ISL 2006-02.

    c. Information coming to the ITP's attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations must to be reported to the nearest Federal Bureau of Investigation (FBI), with a copy to the CSA, in accordance with 32 CFR §117.8 (b), and ISLs 2006-02 and 2013-05.

    d. Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately to the CSA per 32 CFR §117.8 (d).

g. Establish a system or process to identify patterns of negligence or carelessness in handling classified information, in accordance with § 117.18 (b)(4), even for incidents that do not warrant a culpability or incident report.

h. Conduct self-inspections of the Insider Threat Program in accordance with §117.7 (h)(2).

i. Oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats.

j. Establish and manage all implementation and reporting requirements, to include self-inspections and independent assessments, the results of which shall be reported to the Senior Management Official.

REMINDERS AND TIPS

- While not a NISPOM rule requirement, when a classified contract includes provisions for CUI training, contractors must comply with those contract requirements.
- Modify roles to accurately reflect capability and complexities of the insider threat program.
- Roles required for companies with classified information systems include:
    - Insider Threat Program Senior Official (ITPSO)
    - Information System Security Manager (ISSO)
    - Facility Security Officer (FSO)
    - Senior Management Official (SMO)
    - Legal Advisor
- An ITPSO may also function as FSO, Chief Information Security Officer (CISO), or other roles.
- This sample will only contain an example for the ITPSO role needed for any ITP. Develop a similar section for ITP organization capabilities and address how each component's program functions.
- Be sure to include that the Senior Management Official (SMO) has self-certified this program plan and provided self-certification by either letter, email, or other written documentation by a specified date to the industrial security representative within the first six months of the implementation phase. Indicate that a full plan will be made available to DCSA upon request for the security rating and review process.

RESOURCES

- Insider Threat Toolkit: **https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/**
- DCSA Security Review and Rating Process (Webinar): **https://www.cdse.edu/Portals/124/Documents/webinars/webinar-understanding-dcsa-review-process-slides.pdf?ver=LVMr4dtFfoe-69v_BDyeRA%3D%3D**
- Insider Threat Program for Industry (Job Aid): **https://www.cdse.edu/Portals/124/Documents/jobaids/insider/insider-threat-job-aid-for-industry.pdf**
- Insider Threat Overview for Facility Security Officers (Video): **https://www.cdse.edu/Training/Security-Training-Videos/Industrial-Security/Insider-Threat-Overview-for-FSOs/**

CDSE Center for Development of Security Excellence

LEARN. PERFORM. PROTECT.