Insider Threat Program

version

Dimitry Dukhovny

March 18, 2024

Contents

Insider Threat Program **1**

1 Purpose 1

2 Scope 1

3 Principles 1

4 Policy 1

5 Responsibilities 1

5.1 Standing Responsibilities 2

5.2 Conditional Responsibilities 2

5.3 Endnotes 2

6 Training Requirements 2

6.1 ITPSO Training 2

6.2 ITP Supporting Personnel Training 3

6.3 Employee ITP Training 3

6.4 ITP Training Records 3

7 Reporting Requirements 3

8 Appendix: Personnel Assignments 4

8.1 ITPSO 4

8.2 ITP Supporting Personnel 4

9 Appendix: Adjudicative Guidelines for Personnel 4

9.1 Allegiance to the U.S. 4

9.2 Foreign Influence 4

9.3 Foreign Preference 5

9.4 Sexual Behavior 5

9.5 Personal Conduct 5

9.6 Financial Considerations 5

9.7 Alcohol Consumption 5

9.8 Drug Involvement 5

9.9 Psychological Conditions 6

9.10 Criminal Conduct 6

9.11 Handling Protected Information 6

9.12 Outside Activities 6

9.13 Use of Information Technology 6

10 Appendix: References 6

Indices and tables **6**

Insider Threat Program

1 Purpose

This plan establishes policy and assigns responsibilities for the portion of Firm's personnel reliability program that applies to its contractually obligated Insider Threat Program (ITP).

The ITP establishes a secure operating baseline for personnel, facilities, information, equipment, networks, or systems from insider threats.

An insider threat is defined as "the likelihood, risk or potential that an insider will use his or her authorized access, wittingly or unwittingly to do harm to the security of the United States."

Insider threats may include harm to Firm or program information to the extent that the information impacts the firm or agency's obligations to protect classified national security information.

The program will gather, integrate, and report relevant and credible information covered by the 13 personnel security adjudicative guidelines that may be indicative of a potential or actual insider threat to deter all Firm employees granted personnel clearances (PCLs) and all employees being processed for PCLs, from becoming insider threats; detect any cleared person with authorized access to any government or Firm resources to include personnel, facilities, information, equipment, networks, or systems, who pose a risk to classified information; and mitigate the risk of an insider threat as defined above.

2 Scope

This ITP Plan applies to all staff offices, regions, and personnel with access to any government or Firm resources to include personnel, facilities, information, equipment, networks, systems, or the supply chain for the same.

3 Principles

Firm is subject to insider threats and will take actions to mitigate or eliminate those threats. Firm will integrate information from government sponsors to continually identify and assess threats to the organization and its personnel and implement programs to defeat the threats.

4 Policy

The ITP will be established to protect personnel, facilities, and automated systems from insider threats in compliance with DoD 5220.22-M *National Industrial Security Program Operating Manual (NISPOM)*.

This program will seek to prevent espionage, violent acts against the Nation or the unauthorized disclosure of classified information; deter cleared employees from becoming insider threats; detect employees who pose a risk to classified information systems and classified information; 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 *NISPOM* paragraph 1-202 with additional guidance provided in Industrial Security Letter (ISL) 2016-02 and Defense Security Service (DSS) *ODAA Process Manual for Certification and Accreditation of Classified Systems under the NISPOM*.

The responsibilities outlined in 5 Responsibilities are designed to enable the ITP to gather, integrate, centrally analyze, and respond appropriately to key threat-related information.

The ITP will consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, and civil liberties issues – including, but not limited to, the use of personally identifiable information (PII) – are appropriately addressed.

5 Responsibilities

Insider Threat Program Senior Official (ITPSO), is designated in this document, to be superceded only by memorandum from the Chief Executive Officer of Firm 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 e-FCL in accordance with cognizant security agency (CSA) guidance and with *NISPOM* 1-202b.

The ITPSO will be responsible for daily operations, management, and ensuring compliance with the minimum standards derived the *NISPOM*.

5.1 Standing Responsibilities

1. Self-certify the Insider Threat Program Plan in writing to DSS no later than 6 months from the issue date of Change 2 to DoD 5220.22-M, *NISPOM*.
2. Provide copies of the Insider Threat Plan upon request and will make the plan available to the DSS during the Security Vulnerability Assessments (SVA).
3. Establish an Insider Threat Program based on the organization's size and operations.
4. Provide Insider Threat training for Insider Threat Program personnel and awareness for cleared employees.
5. Conduct self-inspections of the Insider Threat Program in accordance with *NISPOM* 1-207b.
6. Oversee the collection, analysis, and reporting of information across the company to support the identification and assessment of insider threats.
7. Establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to the Firm executive team to meet CSA contractual reporting requirements.

5.2 Conditional Responsibilities

1. When Firm has privileged or unprivileged access to CSA systems or systems authorized by a CSA to process government information, 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 as per the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), and Committee for National Security Systems (CNSS) and in accordance with *NISPOM* 8-100d.
2. When Firm assigns personnel to visit, work in, or work with materials owned by a U.S. government CSA, establish procedures in accordance with *NISPOM* 1-202b and 1-300, to access, gather, integrate, and provide for reporting of relevant and credible information across the contractor facility, such as human resources, security, information assurance, and legal review, covered by the 13 personnel security adjudicative guidelines [1] that may be indicative of a potential or actual insider threat to deter employees from becoming insider threats; detecting insiders who pose a risk to classified information; and mitigating the risk of an insider threat.
3. When Firm assigns personnel to visit, work in, or work with materials owned by a U.S. government CSA, establish a system or process to identify patterns of negligence or carelessness in handling classified information, in accordance with *NISPOM* 1-304c, even for incidents that do not warrant a culpability or incident report.

5.3 Endnotes

1 Allegiance to the U.S., Foreign Influence, Foreign Preference, Sexual Behavior, Personal Conduct, Financial Considerations, Alcohol Consumption, Drug Involvement, Psychological Conditions, Criminal Conduct, Handling Protected Information, Outside Activities, Use of Information Technology,

6 Training Requirements

6.1 ITPSO Training

1. The ITPSO shall complete training within 30 days of the authorization of this document.

2. If Firm appoints a new ITPSO after the 6-month implementation period, the new ITPSO will complete the required training within 30 days assignment to ITPSO responsibilities.

6.2 ITP Supporting Personnel Training

1. All personnel assigned duties related to insider threat program management will attend the training outlined in *NISPOM* 3-103a and ISL 2016-02.
    - Counterintelligence and security fundamentals, including applicable legal issues.
    - Procedures for conducting insider threat response actions.
    - Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.
    - Applicable legal, civil liberties, and privacy policies.
2. After initial implementation of this plan and completion of the required training, all new Firm personnel assigned duties related to the ITP management will complete the above training within 30 days of being assigned duties and refresher training annually thereafter.

6.3 Employee ITP Training

1. Firm requires training on insider threat awareness in accordance with *NISPOM* 3-103b for all cleared employees before being granted access to classified information and annually thereafter in accordance with *NISPOM* 3-103b.
    - The importance of detecting potential Insider Threats by cleared employees and reporting suspected activity to the Insider Threat Program designee.
    - Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems
    - Indicators of Insider Threat behavior, and procedures to report such behavior.
    - Counterintelligence and security reporting requirements, as applicable.
2. Cleared employees already in access will complete insider threat awareness training no later than 30 days after assignment to Firm duties with CSA systems or resources and annually thereafter in accordance with *NISPOM* 3-103b.
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 *NISPOM* 3-103b.

6.4 ITP Training Records

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 *NISPOM* 3-103c.
2. Insider threat training records will maintain records of all employee insider threat awareness or program initial and refresher training in accordance with *NISPOM* 3-103c.
3. Insider Threat Training Records will be available for review during DSS security vulnerability assessments, as applicable.
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 *NISPOM* 3-108.
5. Employees shall report training conducted at CSA sites with issued certificates of training or certifying memoranda, if certificates are unavailable.

7 Reporting Requirements

All Firm personnel shall coordinate and share all credible insider threat information with the ITPSO, which will then take action as directed in *NISPOM* 1-300.

Reportable information includes:

1. 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 as in 9 Appendix: Adjudicative Guidelines for Personnel, which must be reported when their observation constitutes adverse information, in accordance with *NISPOM* 1-302a, ISL 2006-02, and ISL 2011-4.
2. Incidents that constitute suspicious contacts, in accordance with *NISPOM* 1-302b and ISL 2006-02.
3. 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) or credentialed CSA counterintelligence personnel, in accordance with *NISPOM* 1-301, ISL 2006-02, and ISL 2013-05.
4. Information determined to be any possible or potential successful penetration of a classified information system must be reported immediately to the CSA per *NISPOM* 1-401.

8 Appendix: Personnel Assignments

8.1 ITPSO

As of the authorization signature on this document, the only company officer or officers authorized to act as ITPSO for Firm are the below-named individual or individuals. Any registration in e-FCL of the firm's KMP shall list the same. Firm directs such named individuals to implement *NISPOM* guidance for the firm as prescribed by each CSA's acquisition team and contracting officer security representative.

The named company officer shall complete training as prescribed under ITPSO Training in 6 Training Requirements.

Role	Name	Telephone	E-mail
ITPSO			

8.2 ITP Supporting Personnel

As of the authorization signature on this document, the following supporting personnel shall complete the ITP Supporting Personnel Training as prescribed in 6 Training Requirements and perform duties as delegated by the ITPSO.

Role	Name	Telephone	E-mail
AITPSO			
AITPSO			

9 Appendix: Adjudicative Guidelines for Personnel

9.1 Allegiance to the U.S.

- An individual must be of unquestionable allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

9.2 Foreign Influence

- Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should cons ider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether

the foreign country is known to target United States citizens to obtain protected informat ion and/or is associated with a risk of terrorism.

9.3 Foreign Preference

- When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

9.4 Sexual Behavior

- Sexual behavior that involves a criminal offense indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in the Guideline may be raised solely on the basis of the sexual orientation of the individual. Some sexual behavior can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information.

9.5 Personal Conduct

- Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:
    - Refusal, or failure without reasonable cause, to undergo or cooperate with security processing, such as meeting with an investigator, completing security forms or releases, cooperating with medical or psychological evaluation.
    - Refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination

9.6 Financial Considerations

- Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.

9.7 Alcohol Consumption

- Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses; and can raise questions about an individual's reliability and trustworthiness.

9.8 Drug Involvement

- The use of illegal drugs or misuse of prescription drugs can raise questions about an individual's reliability and trustworthiness, both because drug use may impair judgment and because it raises questions about an individual's willingness to comply with laws, rules, and regulations.

9.9 Psychological Conditions

- Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional – such as a clinical psychologist or psychiatrist – employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

9.10 Criminal Conduct

- Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness and calls into question a person's ability or willingness to comply with laws, rules, and regulations.

9.11 Handling Protected Information

- Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information and is a serious security concern.

9.12 Outside Activities

- Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

9.13 Use of Information Technology

- Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

10 Appendix: References

Title	Notes
DOD 5220.22-M NISPOM	National Industrial Security Program Operating Manual
ISL 2016-02	Insider Threat Minimum Standards for Contractors
CDSE Insider Threat Training	DOD ITP Management Personnel Training Requirements and Resources
Personnel Adjudicative Guidelines	CDSE list and specification of valid adjudication criteria

Indices and tables

- **genindex**
- **modindex**
- **search**