CDSE
Center for Development of Security Excellence

INDUSTRIAL SECURITY
JOB AID

Standard Practice Procedures (SPP)

Per the 32 Code of Federal Regulations (CFR), Part 117, National Industrial Security Program Operating Manual (NISPOM), a Standard Practice Procedure (SPP) is a document prepared by a contractor that implements the applicable requirements for the contractor's operations and involvement with classified information at the contractor's facility. DCSA released Industrial Security Letter, or ISL, 2021-02, providing guidance regarding reporting requirements for cleared contractors per Security Executive Agent Directive 3, or SEAD 3. One of the requirements is a written plan or SPP; below is a list of items to include in the SPP, both required and as a best practice.

This job aid is to assist in creating an SPP and not a template. Every SPP must be tailored to facility operations, including how the company functions, physical location, classified work performance, and any unique challenges.

Tips: Include best practice information in the SPP, as it is better to establish written procedures in advance than determining what to do upon incident.

1) Opening Statement

State the purpose of the SPP, including a statement of support for the National Industrial Security Program (NISP). The SPP is required to be signed by the Senior Management Official to show management support and make the SPP official.

Think About It: Security is a collaborative process. When creating the SPP, work with other functional managers to coordinate policies. For example, coordinate with HR for employee status changes and IT for suspicious email reporting.

Tips: Brief the SPP contents to all employees, both cleared and uncleared.

RESOURCES:

Facility Clearances in the NISP (IS140.16) https://www.cdse.edu/Training/eLearning/IS140/

2) Facility Information

State the Facility Security Clearance (FCL) level, the storage requirements (if applicable), and whether the company is under a Foreign Ownership Control or Influence (FOCI) mitigation agreement. List the required Security Roles:

- Senior Management Official (SMO): NISPOM 117.7b (1) (iii) and 117.7b (2)

Responsible for policy and strategy, the SMO is the ultimate authority over the facility's operations. The SMO appoints the Facility Security Officer (FSO) and Insider Threat Programs Senior Official (ITPSO) and must remain fully informed of the facility's classified operations.

RESOURCES:

Industrial Security for Senior Management Short
https://securityawareness.usalearning.gov/cdse/multimedia/shorts/issm/story_html5.html

- Facility Security Officer (FSO): NISPOM 117.7b (1) (iii) and 117.7b (3)

  Supervises and directs the security measures necessary to meet NISPOM and classified contract requirements to ensure the protection of classified information.

Tips: The Assistant Facility Security Officer (AFSO) should also complete FSO training.

RESOURCES:

FSO Orientation for Non-Possessing Facilities (IS020.CU):
https://www.cdse.edu/Training/Curricula/IS020/

FSO Program Management for Possessing Facilities (IS030.CU):
https://www.cdse.edu/Training/Curricula/IS030/

- Insider Threat Programs Senior Official (ITPSO): NISPOM 117.7b (1) (iii) and 117.7b (4) Establishes and manages the insider threat program.

RESOURCES:

Insider Threat Training Product Catalog
https://www.cdse.edu/Training/Insider-Threat/

3) Personnel Security Clearances (PCL) (NISPOM 117.10)

Employees - An employee is processed for a PCL only if it is determined that access is essential to fulfill the work performance of a classified contract (NISPOM 117.10a (1) (i)). U.S. citizenship is verified, and the employee will accurately complete an SF86. The FSO will inform the employee in writing that the SF86 review is only for adequacy and completeness and no other purpose within the company. Fingerprints are submitted with the PCL application. Once an employee receives initial eligibility, there is automatic enrollment in Continuous Vetting (CV). CV is the process that regularly reviews a cleared individual's background to ensure they continue to meet security clearance requirements and hold a position of trust. Every employee with access will fill out an SF86 every five years regardless of PCL level.

Consultants - A consultant is an individual under contract to provide professional or technical assistance in a capacity requiring access to classified information. The consultant executes a Consultant Agreement that outlines specific security responsibilities.

Tips: Create a PCL Justification Form to verify a need-to-know. The number of employees processed for a clearance must be limited to the minimum necessary for operation efficiency.

RESOURCES:

Personnel Clearances in the NISP (IS142.16):
https://www.cdse.edu/Training/eLearning/IS142/

SEAD 4, National Security Adjudicative Guidelines and SEAD 6, Continuous Evaluation:
https://www.cdse.edu/Training/Toolkits/Personnel-Security-Toolkit/

4) Reporting Requirements: NISPOM 117.8, SEAD 3, ISL 2021-02

The SPP must establish the necessary processes and procedures to inform cleared personnel on reporting requirements related to SEAD 3 and adverse information. Examples of SEAD 3 required reporting are unofficial foreign travel, contacts, and affiliations; behavioral concerns; media contact; criminal activity; alcohol or drug-related treatment; or financial concerns.

Specifically, the SPP must answer the following questions:

1. Detail how the company will receive, process, and manage the required reports from cleared individuals.
2. How these processes and procedures will be implemented at the company.
3. How covered individuals will alert the company of reportable actions on themselves and concerning other covered individuals.

Types of reporting:

- Adverse Information (NISPOM 117.8 (c) (1)) - any information regarding a cleared employee that suggests their ability to safeguard classified information may be impaired or the individual presents an insider threat concern. Adverse information must be reported in the database of record.
- Unofficial Foreign Travel (SEAD 3, ISL 2021-02) - required to be reported and approved before travel and must include the itinerary. The traveling employee will receive a pre- and post-travel briefing.

- Cleared Employee Status Changes (SEAD 3, NISPOM 117.8 (c) (3)) - must be reported in the database of record. Examples are a change in name, employment, citizenship, marital status, or death.
- Espionage/Sabotage (NISPOM 117.8 (a) (2) (iii) and 117.8 (b)) - Your SPP must document how to report incidents of espionage and/or sabotage to the appropriate government channels.
- Suspicious Contacts (NISPOM 117.8 (c) (2)) - A suspicious contact is the attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure. This includes unclassified information related to export control information, company proprietary information, and Controlled Unclassified Information (CUI). Report all suspicious contacts to the DCSA.
- Security Incidents and Violations (NISPOM 117.8 (d) and NISPOM 117.8(e)):
  - A security infraction is a security incident that does not result in the loss, compromise, or suspected compromise of classified information. However, a security infraction incident may require a report being submitted in the database of record, based on SEAD 3 and SEAD 4 requirements.
  - A security violation is a security incident that reasonably could result or did result in the loss, compromise, or suspected compromise of classified information. Conduct a preliminary inquiry, then submit an initial report and a final investigation report to DCSA. Submit a culpability report in the database of record for persons found responsible for a security violation.
  - Create and apply a graduated scale of administrative discipline in the event of employee security violations, infractions, or other issues of negligence related to the NISP, per NISPOM 117.8(e)(2). In addition, you are required to establish a system to track information regarding employees who are the subject of a security violation, per NISPOM 117.8(e) (1).

Tips: Include in the SPP the direct contact information of whom the employee is to report. You can also post this information in the facility.

Think About It: Create a culture of self-reporting of adverse information before it is discovered by DCSA during CV.

Think About It: Security education is one of the most effective ways to mitigate security vulnerabilities. Cleared employees must understand reporting is required not only for themselves but also other cleared employees. Provide security education to both cleared and uncleared employees, including how to report suspicious contacts.

RESOURCES:

Reporting Requirements Job Aid:
https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/CDSE_RR_JobAid.pdf

SEAD 3 Industry Reporting Desktop Job Aid:
SEAD-3_Reporting_Desktop_Aid_for_Cleared_Industry-revisedMarch2022.pdf (dcsa.mil)

SEAD 3 Unofficial Foreign Travel Reporting:
https://www.dcsa.mil/mc/isd/sead3_foreign_travel/

Targeting U.S. Technologies: A Report of Threats to Cleared Industry: (Additional Resources, Reports Tab): https://www.dcsa.mil/Counterintelligence-Insider-Threat/

Method of Contact/Method of Operation Matrix Video:
https://m.youtube.com/watch?v=r7lMqikT_R8

Security Incident Job Aid:
https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/security-incident-job-aid.pdf

5) FCL Changed Conditions: NISPOM 117.8 (c) (7) (8) (9)

If there are changes in your company, it is a requirement to report this to DCSA through the system of record. Examples include change of ownership; change in foreign ownership, control, or influence (FOCI); change of Key Management Personnel (KMP); change of business name; and termination of business. If the company stores classified information, it also must be reported if there is a change in storage capability and inability to safeguard classified information.

6) Insider Threat Program: NISPOM 117.7 (d), 117.12 (g)

Insider threat is 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. The contractor will establish and maintain an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat. Create an effective Insider Threat Plan and provide training to insider threat program personnel. Training must be documented and given to all cleared employees before granting classified access and annually thereafter, including:

- The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the ITPSO.
- Methodologies of adversaries to recruit trusted insiders and collect classified information, including information systems.
- Indicators of insider threat behavior and procedures to report such behavior.

- CI and security reporting requirements, as applicable.

Think About It: Functional managers should take Establishing an Insider Threat Program for Your Organization (INT122.16), as they have a role in identifying and mitigating insider threat issues.

RESOURCES:

Establishing an Insider Threat Program for Your Organization (INT122.16): https://www.cdse.edu/Training/eLearning/INT122/

7) Security Education: NISPOM 117.12

Contractors will keep records of the date of the most recent training for cleared employees as well as the type of training provided.

- Initial Briefing - All cleared employees must receive an initial security briefing and sign a Nondisclosure Agreement (SF 312) prior to having access to classified material. The initial security briefing must include:
  - Threat awareness (includes insider threat)
  - Counterintelligence awareness
  - Overview of the security classification system
  - Employee reporting obligations and requirements (includes insider threat)
  - Cybersecurity training for all authorized information system users
  - Security procedures and duties applicable to the employee's position
- Refresher Briefing - All cleared employees must receive an annual refresher training every 12 months that reinforces the information provided during the initial training and address any issues identified during the self-inspection. When a classified contract includes security and training requirements for CUI, contractors must comply with those requirements.
- Derivative Classification - Employees who have been authorized to make derivative classification decisions must complete initial derivative classification training beforehand and refresher training at least once every two years.
- Debriefings - When classified access is no longer required or employment is terminated, employees are required to be debriefed.

Tips: Ideally, you can have employees sign the debriefing statement on the SF312.

Think About It: There may be special access requirements on the classified contract, such as Communications Security (COMSEC), North Atlantic Treaty Organization (NATO), and Critical Nuclear Weapon Design Information (CNWDI). Provide any required briefings and debriefings as required in the NISPOM.

RESOURCES:

CDSE Industrial Security:
https://www.cdse.edu/Training/Industrial-Security/

CDSE CI Toolkit:
https://www.cdse.edu/Training/Toolkits/Counterintelligence-Awareness-Toolkit/

8) Self-Inspections (Contractor Reviews): NISPOM 117.7 (h)(2)

Review the security program on a continuing basis and conduct a formal self-inspection at least annually. The purpose is to assess the security procedures to determine the effectiveness and identify any deficiencies in the security program consistent with risk management principles and NISPOM requirements. A self-inspection should include conducting employee interviews to verify general understanding of the security requirements. Prepare a formal report describing the results of the self-inspection, its findings, and resolution of issues discovered. Retain this formal report for DCSA to review. The SMO will annually certify to DCSA, in writing, that a self-inspection has been conducted, that other Key Management Personnel (KMP) have been briefed on the results, that appropriate corrective actions have been taken, and that management fully supports the security program.

Tips: Include SPP review as part of the self-inspection and update as needed.

Think About It: The self-inspection and the DCSA security review both assess the strength of the security program and identify and correct vulnerabilities. An effective and thorough self-inspection can result in a positive DCSA security review.

RESOURCES:

Self-Inspection Handbook for NISP Contractors (Self-Inspections Training tab):
https://www.cdse.edu/Training/Toolkits/FSO-Toolkit/

NISP Self-Inspection (IS130.16):
https://www.cdse.edu/Training/eLearning/IS130/

9) Classified Visits and Meetings: NISPOM 117.16

The number of classified visits will be held to a minimum and approved in advance. Determine if the visit is necessary and cannot be achieved without access to, or disclosure of, classified information. Establish procedures to ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. Only afford classified access consistent with the purpose of the visit. For outgoing classified visits, provide company FCL and employee PCL information, the name of the person to be visited, the time and duration of the visit, and the justification for the visit. Process outgoing visits in the database of record or by submitting a Visit Authorization Letter (VAL) document.

Tips: Have a visitor log for all visitors that includes citizenship, including unclassified visits. Use badges to identify visitors.

Think About It: If your company is under a FOCI mitigation agreement, you may have a separate requirement for visitations between the foreign parent and the company. If you do, include a section to define the requirements to the employees.

RESOURCES:

Visits and Meetings in the NISP:
https://www.cdse.edu/Training/eLearning/IS105/

FOR FACILITIES WITH SAFEGUARDING

10) Safeguarding Classified Information: NISPOM 117.15

Contractors are responsible for properly safeguarding classified information. If your company does not have classified materials onsite, then these requirements will not apply. Establish procedures for these areas:

- End-of-day checks - Describe how your facility will complete end of day checks as required.
- Oral Discussions - Ensure classified discussions will not take place over unsecure telephones, email, public places, or in any other manner that permits interception by unauthorized persons by creating the appropriate policies.
- Perimeter Controls - Deter and detect unauthorized introduction or removal of classified material from the facility. Post a sign at all pertinent entrances stating that all persons who enter or exit the facility will be subject to random inspection of their personal effects.
- Incoming Classified Material - A cleared, authorized individual must receive all incoming classified material.

- Transmission of Classified Information - Include procedures related to couriers and the use of approved Government Services Administration (GSA) overnight commercial companies for domestic express delivery services for the transmission of Secret and Confidential material.
- Reproduction of Classified Material - Classified reproduction should only take place on approved Information Systems (IS) and approved copy machines.
- Destruction of Classified Material - Minimize the amount of classified material to the amount consistent with contractual performance. Return classified material to the government customer or prime contractor once the contract is complete.
- Retention of Classified Materials - Typically, contractors may retain classified materials for two years after the conclusion of the classified contract. Retention authority must be requested in writing to the government customer before two years has passed.
- Combinations - Authorized persons should memorize the combinations for all GSA classified security containers onsite. If a written record of the combination is needed, it will be marked and safeguarded in accordance with the highest level of material stored in the container. Change combinations when the following events occur: upon receiving the approved container or lock; the reassignment, transfer, termination of employment, PCL downgrade, or termination of a PCL for any person having knowledge of the combination; the compromise or suspected compromise of a container or its combination, or the discovery of a container left unlocked or unattended.
- Public Release/Disclosure - Do not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and approval by the government customer.
- Emergency Procedures - In emergencies, it is important to safeguard all classified information as best as possible. However, the overriding consideration in any emergency is the safety of personnel. Report to DCSA any emergency that renders their location incapable of safeguarding classified material as soon as possible. Include emergency contact information.

Tips: It is required to perform end-of-day security checks. Consider using Standard Form(s) 701 and 702 to record end of day checks and GSA container open and close records. In addition, it is recommended to document all random perimeter inspections conducted.

Tips: In addition to emergency procedures regarding classified information, include building emergency procedures in your SPP to consider the safety of all employees.

Tips: Even if your company does not store classified information onsite, if employees access classified information at other locations, it is important to remind them to follow the procedures and guidelines for that facility.

Think About It: DCSA will not grant safeguarding approval until procedures are in place, including emergency procedures.

RESOURCES:

Safeguarding Classified Information in the NISP (IS109.16):
https://www.cdse.edu/Training/eLearning/IS109/

Handling Classified Information Flowchart:
https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/IS109-SFG03-Handling.pdf?ver=_kUn2PBCducjunmyxdse5Q%3d%3d

Storage Requirements by Classification Level:
https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/IS109-SFG04-Storage.pdf?ver=HciNRrR4ErO_lIBZlaUzGg%3d%3d

11) Marking Classified Information: NISPOM 117.14

Describe procedures on how all classified information would be marked based on the contractual requirements stated in the Security Classification Guidance (SCG). End-of-day checks - Describe how your facility will complete end of daychecks as required.

- Classification Levels
    - Confidential - Information that if compromised could cause "Identifiable" damage to national security.
    - Secret - Information that if compromised could cause "Serious" damage to national security and requires a substantial degree of protection.
    - Top Secret - Information that if compromised could cause "Exceptionally Grave" damage to national security and requires the highest degree of protection.
- Working Papers - Working papers containing classified information will be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed. Working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level if released outside of the facility, filed permanently, or retained for more than 180 days.

- Derivative Classification - Employees authorized to perform derivative classification actions must have adequate training and the proper SCG necessary to accomplish these actions.
  CUI - Train employees on CUI marking requirements when CUI requirements are called for in a classified contract. CUI must be stored in a secured manner.

RESOURCES:

Marking Classified Information
https://www.cdse.edu/Training/Marking-Classified-Information/

Derivative Classification
https://www.cdse.edu/Training/Derivative-Classification/