Lesson 1: Course Introduction

Course Information

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Provide an overview of the Facility Security Officer’s (FSO) primary roles in the National Industrial Security Program (NISP) and introduce the resources the FSO will work with to meet the requirements of the NISP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>FSOs, Defense Security Service (DSS) Industrial Security Representatives, and others involved in the NISP</td>
</tr>
<tr>
<td>Pass/Fail %</td>
<td>Unlike most other courses, there is no separate test to pass to receive credit for this course. Instead, students must visit every screen and complete 100% of the practical exercises to receive credit for passing this course.</td>
</tr>
<tr>
<td>Estimated completion time</td>
<td>215 minutes</td>
</tr>
</tbody>
</table>

Course Overview

To preserve and protect our national security, the U.S. government must safeguard its secrets. How can the government meet this important responsibility when there are so many U.S. companies and industry employees who have access to those secrets? The answer is the National Industrial Security Program (NISP), a government-industry partnership that protects the millions of classified documents being held by contractors.

Key players in this program are the Facility Security Officers (FSOs), designated to represent each cleared facility, and responsible for ensuring that their facilities comply with government requirements. Since the FSO is the primary representative of the company for security matters, it is important for the FSO to have full support from the senior management official and other key management personnel of the facility.

This course will demonstrate the importance of a partnership between the FSO and the government. Effective security management for the protection of our nation’s
secrets depends on it. The FSO roles introduced in this course will be explored in more depth in the other courses in the FSO curriculum.

Course Objectives

- Identify the purpose of the National Industrial Security Program (NISP)
- Identify roles and responsibilities in the NISP
- Identify the structure and requirements of the National Industrial Security Operating Manual (NISPOM)
- Identify and access resources available to the Facility Security Officer (FSO)
- Identify government personnel who will work with the FSO to meet the requirements of the NISP

Course Structure

- Course Introduction
- Roles and Responsibilities
- Policy Guidance and Reporting Requirements
- Resources
- Final Learning Activity
- Course Conclusion
Lesson Introduction

The National Industrial Security Program (NISP) is a government-industry partnership forged to help protect our national security. As a Facility Security Officer (FSO) you play a pivotal role in this program. But you are not alone with this important responsibility. Many government employees, organizations, agencies, and employees of your own company are available to support you. To be effective as an FSO, you need to understand what the NISP is, and who the participants are. You also need to understand each player’s roles and responsibilities, including your own crucial role, in the NISP.

The lesson objectives are to be able to:

- Identify the purpose of the National Industrial Security Program (NISP)
- Identify the roles of the Facility Security Officer (FSO) in the NISP
- Identify government roles and responsibilities in the NISP
- Identify the four Cognizant Security Agencies (CSAs) in the NISP
- Identify the Cognizant Security Office (CSO) for the Department of Defense (DoD)
- Identify the functions of the Defense Security Service (DSS)
- Identify people, government organizations, and government agency websites that can provide resources to the FSO

NISP Overview

Purpose of the NISP

The purpose of the NISP is to safeguard classified information entrusted to industry.

What exactly is classified information? Classified information is any official U.S. government information that an authorized U.S. government official has determined must be protected in the interest of national security. The authorized official that makes this determination is known as the original classification authority.
Why is it so important to protect this information? In a world where information is key, protecting information is far more than protecting words on paper or bits on a computer. Protecting classified information means protecting our resources and intellectual property, protecting the lives of our military personnel, protecting our national security, and protecting our very way of life. Keep these images in mind as you implement the NISP at your facility.

**Origins of the NISP**

Why does classified information need to be protected in industry? Let’s consider how the NISP got started. The federal government has always purchased goods and services from the private sector. Sometimes a company needs access to classified information to fulfill the terms of a government contract. Other times, classified information is generated within industry as part of a collaborative relationship between the government and industry.

Regardless of how classified information is generated, the federal government owns or legally controls it. The government requires that classified information be protected.

In the past, each government agency or department established its own standards for protecting classified information in industry. Then, in January 1993, President Bush signed Executive Order 12829, mandating the establishment of one national program, so that all federal agencies would use one set of rules to protect classified information related to federal contracts with industry. This program is the National Industrial Security Program.

**Classification Levels**

Let’s look briefly at the system used for classifying information. The system for classifying, safeguarding, and declassifying national security information is mandated by Executive Order 13526. The Atomic Energy Act of 1954 also establishes legal authority to classify information. Under this system, classified information is designated at one of three levels, based on the extent of damage to national security that could occur if the information were compromised. The handling and safeguarding requirements are different for each classification level.
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidential</strong></td>
<td>Unauthorized disclosure of Confidential information could cause <strong>damage</strong> to national security; for example, by:</td>
</tr>
<tr>
<td></td>
<td>- Revealing the strength of our armed forces</td>
</tr>
<tr>
<td></td>
<td>- Revealing technical information about weapons, such as:</td>
</tr>
<tr>
<td></td>
<td>- Performance characteristics</td>
</tr>
<tr>
<td></td>
<td>- Test data</td>
</tr>
<tr>
<td></td>
<td>- Design</td>
</tr>
<tr>
<td></td>
<td>- Production data</td>
</tr>
<tr>
<td></td>
<td>- Revealing other information that would cause damage</td>
</tr>
<tr>
<td><strong>Secret</strong></td>
<td>Unauthorized disclosure of Secret information could cause <strong>serious damage</strong> to national security; for example, by:</td>
</tr>
<tr>
<td></td>
<td>- Significantly impairing a program or policy directly related to national security</td>
</tr>
<tr>
<td></td>
<td>- Revealing significant military plans or intelligence operations</td>
</tr>
<tr>
<td></td>
<td>- Compromising significant scientific or technological development related to national security</td>
</tr>
<tr>
<td><strong>Top Secret</strong></td>
<td>Unauthorized disclosure of Top Secret information could cause <strong>exceptionally grave damage</strong> to national security; for example, by:</td>
</tr>
<tr>
<td></td>
<td>- Disrupting vital relations with other countries</td>
</tr>
<tr>
<td></td>
<td>- Compromising vital defense plans</td>
</tr>
<tr>
<td></td>
<td>- Compromising cryptologic and communications intelligence systems</td>
</tr>
<tr>
<td></td>
<td>- Jeopardizing sensitive intelligence operations</td>
</tr>
<tr>
<td></td>
<td>- Jeopardizing a vital advantage in an area of science or technology</td>
</tr>
</tbody>
</table>
NISP Roles and Responsibilities

**FSO Roles**

Under the NISP, the government establishes requirements for the protection of classified information in industry, and industry implements those requirements with advice, assistance, and oversight from the government. As your company’s designated FSO, and one of several key management personnel (KMP), you represent your company for all matters related to security. As a liaison between your company and the government, you must ensure that your company’s employees understand and comply with government security requirements. You can help them do so by taking full advantage of the government’s advice and assistance as you perform your duties.

Let’s look more closely at your roles in the NISP. As the FSO, you are responsible for managing the security program under which you will obtain and maintain your company’s facility security clearance and for helping company employees obtain and maintain personnel security clearances. You play an important role in security education, training, and awareness, in threat awareness and counterintelligence, and in helping maintain cyber security awareness and preparedness. You play a critical role in safeguarding classified information, as well as for protecting unclassified export-controlled information relating to your classified contracts and for reporting cyber-attacks relating to this information. You are also responsible for security vulnerability assessments and self-inspections and for reporting certain types of events back to the government.

You are not expected to fill all these roles on your own. Within your own company, there are many individuals and offices that can offer support to your security program, including senior management, human resources, business development, information technology, and the office of export controls, if you have one. Remember that in addition to providing oversight, the government is available to advise and assist you.

Review each role below to learn more.

**Facility Clearance**

Before your company can work with classified materials, it must have a facility security clearance. A facility clearance indicates that your company is eligible for access to information classified at the level of the facility clearance and at any of the lower classification levels. Among other requirements, your company must have sponsorship and execute the DD Form 441, DoD Security Agreement, to obtain its facility clearance. You, as the FSO, must ensure your company
maintains its facility clearance by meeting its contractual obligations for continued compliance with applicable government security requirements.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD Form 441, DoD Security Agreement</td>
<td>A legally binding contract between the DoD and a contractor who will have access to classified information</td>
</tr>
</tbody>
</table>

CDSE offers the following online course for this topic:
- Facility Clearances in the NISP Course

Personnel Clearance

The people in your company must be cleared before they can have access to classified information. Your company’s employees will look to you to help them obtain and maintain their personnel security clearances. Like facility clearances, personnel security clearances are issued at a particular classification level, indicating that an employee is eligible for access to information classified at that level and at any of the lower classification levels. As one of your company’s key management personnel, you must be cleared to the same level as your company’s facility clearance.

CDSE offers the following online course for this topic:
- Personnel Clearances in the NISP Course

Security Education

As an FSO, you must provide an initial briefing to all newly cleared employees. And you must periodically brief your employees on government security requirements and make sure they get the training they need to comply with the National Industrial Security Program Operating Manual (NISPOM). You will learn more about this document later in this course. You should also make sure your company’s employees are aware of potential threats to security, including cyber intrusions on unclassified systems, and understand special requirements for handling certain types of classified information.

CDSE offers the following online courses for this topic:
- Developing a Security Education and Training Program Course
- Counterintelligence and Threat Awareness Course
Safeguarding

Ensuring that your company protects classified materials from unauthorized disclosure is a crucial aspect of your role as FSO. Your specific responsibilities may vary depending on your facility. All cleared employees must understand and abide by government regulations regarding the disclosure of classified information. If your company generates classified material, then your personnel must be trained in proper classification marking procedures. If your company stores classified materials, those materials must be safeguarded at all times. This includes the proper maintenance of classified information systems. If personnel at your company must transmit or transport classified materials, then you must ensure that they do so according to government requirements.

CDSE offers the following online courses for this topic:

- Safeguarding Classified Information in the NISP Course
- Derivative Classification Course
- Marking Classified Information Course
- Transmission and Transportation for Industry Course

Self-Inspection

Government representatives will review your company periodically to make sure it remains in compliance with the requirements of the NISPOM. Your self-inspection supplements the government security vulnerability assessment and helps you to identify areas where you are not in compliance and areas where you must improve your security program. However, by reviewing your security status and conducting required self-inspections, you ensure that you are ready for the government security vulnerability assessments and that your company remains in compliance between government security vulnerability assessments.

CDSE offers the following online course for this topic:

- NISP Self Inspection Course

Reporting

As the FSO, you are responsible for reporting to the government specific types of actions, situations, or status changes relating to the potential compromise of classified information and/or unclassified information relating to your classified programs, to include cyber intrusions on your unclassified systems.

CDSE offers the following online course for this topic:

- NISP Reporting Requirements Course
Government Roles

Policy and Oversight

To make the most of government advice and assistance, you should be familiar with how the NISP is administered on the government side.

Let's start at the top. NISP policy direction is provided by the National Security Council (NSC) which reports to the President.

A separate, independent advisory body called the Information Security Oversight Office (ISOO) is responsible to the President for monitoring how the NISP is implemented. The ISOO issues NISP implementation directives and produces an annual report on the NISP. The ISOO is also responsible for overseeing the system for classifying and declassifying information.

As the Executive Agent of the NISP, the Secretary of Defense is responsible for overall implementation of the program. The Department of Defense (DoD) issues and maintains the NISPOM, inspects and monitors cleared companies who require access to classified information, and determines eligibility for access to classified information.

Four executive branch agencies have been designated as Cognizant Security Agencies (CSAs). Each CSA is responsible for the protection of classified information within its purview in the NISP. The Director of National Intelligence (DNI) retains authority over access to intelligence sources and methods. The Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) each retains authority over access to its own programs. The DoD is the largest CSA, as it has the most contracts with industry. The DoD oversees the NISP not only for its own contracts, but also for industry contracts with approximately 25 other federal agencies. Through memoranda of agreement (MOAs) with the Secretary of Defense, these agencies have agreed to recognize the DoD as their CSA.

<table>
<thead>
<tr>
<th>The DoD is the CSA for the following agencies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Department of Agriculture</td>
</tr>
<tr>
<td>• Department of Commerce</td>
</tr>
<tr>
<td>• Department of Education</td>
</tr>
<tr>
<td>• Department of Health and Human Services</td>
</tr>
<tr>
<td>• Department of Homeland Security</td>
</tr>
<tr>
<td>• Department of the Interior</td>
</tr>
<tr>
<td>• Department of Justice</td>
</tr>
<tr>
<td>• Department of Labor</td>
</tr>
<tr>
<td>• Department of State</td>
</tr>
<tr>
<td>• Department of Transportation</td>
</tr>
<tr>
<td>• Department of the Treasury</td>
</tr>
</tbody>
</table>
The DoD is the CSA for the following agencies:

<table>
<thead>
<tr>
<th>Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>Federal Reserve System</td>
</tr>
<tr>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>General Services Administration</td>
</tr>
<tr>
<td>National Archives and Records Administration</td>
</tr>
<tr>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>National Science Foundation</td>
</tr>
<tr>
<td>Nuclear Regulatory Commission</td>
</tr>
<tr>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>Overseas Private Investment Corporation (OPIC)</td>
</tr>
<tr>
<td>Small Business Administration</td>
</tr>
<tr>
<td>United States Agency for International Development</td>
</tr>
<tr>
<td>United States International Trade Commission</td>
</tr>
<tr>
<td>United States Trade Representative</td>
</tr>
</tbody>
</table>

Administration

Each CSA is authorized to establish an industrial security program for the purpose of safeguarding classified information entrusted to industry. These agencies oversee the NISP, but they may have subordinate elements that administer the program. Such an element is called a Cognizant Security Office (CSO).

CSOs are responsible for administering the NISP on behalf of the CSAs. Each CSA organizes its CSO differently. The DoD has delegated the CSO role for itself and the other agencies under its purview to an agency within the DoD called the Defense Security Service (DSS). As the administrator of the NISP for the DoD and other federal agencies, the DSS will be your primary government point of contact for industrial security-related matters.

DSS Mission Areas

There are two primary mission areas of DSS, which is headquartered in Quantico, Virginia. One is administration of the NISP. Under the NISP, DSS provides security support to the military services, defense agencies, other federal agencies, and approximately 13,000 cleared contractor facilities. The DSS Industrial Security Field Operations (ISFO) which administers the NISP will assign an Industrial Security Representative (IS Rep) to your facility to help you implement NISP requirements.

The other DSS mission area is Security Education, Training and Awareness (SETA) which is administered by the Center for Development of Security Excellence (CDSE) located in Linthicum, Maryland. The mission of the SETA directorate is to serve as a
security center of excellence for the professionalization of the security community and to be the premier provider of security education and training for the DoD and industry.

As a security professional, you will find CDSE to be a very useful resource. You will be able to take advantage of security professionalization, training, and education offered by the CDSE, and you will also be able to use their security awareness products.

SETA is comprised of three divisions:

<table>
<thead>
<tr>
<th>Division</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professionalization</td>
<td>Responsible for the implementation and maintenance of the Security Professional Education and Development Program (SPeD)</td>
</tr>
<tr>
<td>Division</td>
<td></td>
</tr>
<tr>
<td>Training Division</td>
<td>Provides security training to Department of Defense (DoD) and other U.S. Government personnel, employees of U.S. Government contractors and when sponsored by authorized DoD Components, employees of foreign Governments</td>
</tr>
<tr>
<td>Education Division</td>
<td>Offers graduate-level courses designed specifically to develop leaders for the DoD security community</td>
</tr>
</tbody>
</table>

**DSS Functions and the FSO**

Now that you understand the overall missions of the DSS, let's look more specifically at DSS functions and how they will support you in your roles as an FSO. As you have seen, your IS Rep is your partner in the NISP. The DSS function that will support you under the SETA mission is the Center for Development of Security Excellence (CDSE).

The DSS functions that will support you under the National Industrial Security Program (NISP) mission are ISFO, the Personnel Security Management Office for Industry (PSMO-I), the Facility Clearance Branch, the Foreign Ownership, Control or Influence (FOCI) Operations Division, the Counterintelligence (CI) Directorate, the International Division, and the Office of Designated Approving Authority (ODAA). Depending on circumstances, you may work directly with personnel in these functions, or you may coordinate your interactions through your IS Rep. Review each function below to learn more.

**Facility Clearance Branch**

The Facility Clearance Branch processes contractors for facility security clearances, issues facility clearances, and monitors the contractors’ continued eligibility in the NISP. You will interact with the DSS Facility Clearance Branch...
when your company is initially being processed for a facility clearance and any
time there are changes in the facility that might affect that clearance.

**FOCI Operations Division**

The DSS Foreign Ownership, Control, or Influence (FOCI) Operations Division
resolves issues that arise when a facility being processed for a clearance or a
previously cleared facility is subject to foreign ownership, control, or influence. If
your company is subject to foreign ownership, control or influence, your IS Rep
will coordinate your interaction with personnel from this division.

**PSMO-I**

The Personnel Security Management Office for Industry (PSMO-I) processes
requests for and issues personnel security clearances and is located near Ft.
George Meade, Maryland. You may interact with the PSMO-I when there are
issues related to an employee’s personnel clearance.

You will use an automated database system called the Joint Personnel
Adjudication System (JPAS) to communicate most personnel clearance
information to PSMO-I. This includes certain types of changes in personnel
information that you are required to report under the NISP.

**CI Directorate**

The DSS Counterintelligence (CI) Directorate is responsible for reviewing reports
of suspicious contacts that may involve foreign intelligence collection, and for
reporting them to the appropriate authorities when necessary.

Each geographic region has a Region CI Chief who oversees the activities of the
Field CI Specialists (FCIS) within the region. The FCIS assists FSOs in
identifying potential threats to U.S. technology and developing CI awareness and
reporting by company employees. Activities include conducting cyber
notifications so cleared industry is aware of cyber threats to their IT systems and
assisting with malware submissions for industry. You may also find your FCIS
helpful in providing foreign travel briefings and debriefings and CI awareness
education briefings.

The FCIS supports the IS Rep in conducting Advise and Assist visits by providing
advice and guidance in CI best practices, and helps conduct Vulnerability
Assessments of cleared contractors’ CI programs. In support of these CI
activities, the CI Directorate publishes Technology Collection Trends in the U.S.
Defense Industry, an annual report on the foreign intelligence threat to facilities
participating in the NISP. This report is a good source of threat awareness
information you can use when briefing employees of your company.
ODAA
The DSS Office of Designated Approving Authority (ODAA) facilitates the certification and accreditation (C&A) process for information systems at cleared contractor facilities. Your role as protector of classified materials includes the protection of classified information stored electronically. If your company has an information system that is accredited to process classified information, an Information System Security Professional (ISSP) will work with you and your company’s Information System Security Manager (ISSM) on all matters related to its maintenance. Your IS Rep will coordinate your company’s interactions with the DSS ODAA.

CDSE
In addition to the course you are now taking, CDSE provides training to support you in all your roles as an FSO. You can access the CDSE course catalog through the DSS website, and you can enroll yourself or your employees can enroll themselves in on-line training through the CDSE’s STEPP system.

You can also email CDSE directly if you have questions about the FSO curriculum.

Office of the Chief Information Officer
The Office of the CIO provides information systems and telecommunications support across DSS, including the NISP. This office supports and maintains the databases and information systems that you will use as an FSO. The Office of the CIO also provides a call center, known as the DoD Security Service Center. The personnel who staff this service center can help you with technical questions about DSS databases and information systems.

<table>
<thead>
<tr>
<th>Databases an FSO uses</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEPP</td>
<td>The Security Training, Education, and Professionalization Portal (STEPP) is CDSE’s learning management system that allows users to access, manage, and track online courses, schedules, and other learning events.</td>
</tr>
<tr>
<td>e-QIP</td>
<td>Electronic Questionnaires for Investigations Processing (e-QIP) is software provided by OPM that allows employees to enter, update, and transmit information electronically over a secure Internet connection to their security office for review and approval. FSOs’ interface with e-QIP via JPAS.</td>
</tr>
<tr>
<td>ISFD</td>
<td>The Industrial Security Facilities Database (ISFD) is the DoD system of record for facility clearance information.</td>
</tr>
</tbody>
</table>
National Industrial Security Program (NISP)

The DSS Industrial Security Field Operations Program Office, which administers the NISP, is located at DSS Headquarters in Quantico, Virginia. DSS maintains industrial security field offices all over the country, which, for management purposes are grouped into four geographic regions. A Regional Director oversees the operation of all the field offices in his or her region. Each field office is locally managed by a Field Office Chief, and staffed by Industrial Security Representatives (IS Reps).

There are over 200 IS Reps located throughout the country. An IS Rep from a nearby office will be assigned to help you implement NISP requirements. This person will be your partner in developing and maintaining your security program in compliance with the NISP.

International Division

The International Division provides guidance and oversight for cleared U.S. contractor involvement with foreign governments, foreign contractors, and NATO. These duties include security oversight and administration of export-controlled items and U.S. classified information released to foreign entities and the import of foreign-government and NATO classified information held by U.S cleared contractors.

Other Government Agencies

In addition to the DSS, there are many other government resources to help you successfully manage your security program. Many government agencies have information and training products on their websites that can be especially helpful as you prepare training and briefings for your company’s employees and managers. You can access the websites from the Course Resources Page. Review each organization or department below to learn more about its mission and the resources it offers.

Information Security Oversight Office (ISOO)

You have already seen the ISOO, which reports to the President on the NISP. The ISOO produces many useful materials that you will learn more about later in this course.

The ISOO is responsible to the President for policy and oversight of the government-wide security classification system and the NISP.

Useful ISOO resources are listed below:

- Reference documents
- Education and training materials
- Marking Classified National Security Information booklet
- Briefing booklets

**Office of the National Counterintelligence Executive (ONCIX)**

The Office of the National Counterintelligence Executive (ONCIX) is part of the Office of the Director of National Intelligence and is staffed by senior CI and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces various products and resources you might find useful in your security education and threat awareness training.

**Office of Personnel Management (OPM)**

The Office of Personnel Management (OPM) manages the federal government workforce. OPM is also responsible for conducting personnel security investigations. When you help a company employee obtain a security clearance, you send a personnel clearance request through the JPAS to PSMO-I. OPM personnel then perform a background investigation. An OPM Personnel Security Investigator may come to your facility to interview your employees and review relevant records. OPM reports the results of the investigation to the DoD Consolidated Adjudication Facility (DoD CAF), which is responsible for issuing a clearance authorization if the individual is eligible.

**Department of Defense (DoD)**

You may find useful briefing and training materials on the websites of many DoD agencies. Take a few moments to familiarize yourself with these agencies.

<table>
<thead>
<tr>
<th>Agency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Threat Reduction Agency (DTRA)</td>
<td>Safeguards the U.S. from weapons of mass destruction (chemical, biological, radiological, nuclear, and high yield explosives)</td>
</tr>
<tr>
<td>Defense Intelligence Agency (DIA)</td>
<td>Provides military intelligence to warfighters, defense planners, and national security policymakers</td>
</tr>
<tr>
<td>Defense Information Systems Agency (DISA)</td>
<td>Provides information systems security for DoD systems</td>
</tr>
<tr>
<td>National Reconnaissance Office (NRO)</td>
<td>Provides overhead reconnaissance satellites</td>
</tr>
</tbody>
</table>
National Security Agency (NSA) | Provides information assurance services and information and signals intelligence
Interagency OPSEC Support Staff (IOSS) | Helps government organizations develop operations security (OPSEC) programs

**Department of Justice (DOJ)**

The Federal Bureau of Investigation (FBI) is part of the Department of Justice. The FBI website is a great source of current threat awareness material that you can use for briefings. The FBI also sponsors the Counterintelligence Domain Program, through which the FBI provides counterintelligence education to business partners; and InfraGard, a government-industry partnership for sharing information and intelligence. You should consider participating in these programs.

As an FSO, you are required to report certain types of events to the government. In addition to reporting to DSS, some events must be reported through FBI agents in local FBI field offices. You will learn more about reporting requirements later in this course.

**Department of Homeland Security (DHS)**

The Department of Homeland Security (DHS) comprises many organizations, three of which are covered here.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS</td>
<td>Leading a unified effort to secure the U.S. against terrorism and cyber threat</td>
</tr>
<tr>
<td></td>
<td>The DHS website includes information about security threats, as well as links to the Department’s subordinate agencies.</td>
</tr>
<tr>
<td>Immigration and Customs Enforcement (ICE)</td>
<td>Eliminating border vulnerabilities and vulnerabilities in economic, transportation, and infrastructure security</td>
</tr>
<tr>
<td>Organization</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transportation Security Administration (TSA)</td>
<td>Protecting U.S. transportation systems \n\nThe Transportation Security Agency (TSA) website may be especially useful for business travelers or for employees who are responsible for transporting material on public transportation.</td>
</tr>
<tr>
<td>United States Computer Emergency Readiness Team (US-CERT)</td>
<td>Improving the nation’s cybersecurity posture \n\nThe United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation’s cybersecurity posture, coordinates cyber information sharing, and proactively manages cyber risks to the Nation. The US-CERT website provides security publications and resources as well as cyber awareness alerts and tips.</td>
</tr>
</tbody>
</table>

**Department of State (DoS)**

The State Department website provides information that is useful for security education, as well as for helping employees who travel overseas and managers who make international business decisions. The Directorate of Defense Trade Controls (DDTC) is responsible for regulating and controlling the export of military items, services, and information.

If your company manufactures, exports, or sells defense articles, services, or related technical data, you will be required to register your facility on the DDTC website.
**Review Activity**

Try answering the following questions. When you are finished, see the Review Activity Answer Key at the end of this Student Guide to check your answers.

**Question 1**

Which of the following best describes the purpose of the NISP?

*Select the best response.*

- ○ To ensure the use of a standard system for classifying documents
- ○ To safeguard classified information in industry
- ○ To safeguard intellectual property rights in the government
- ○ To ensure that the government contracts with trustworthy industrial partners

**Question 2**

As an FSO, which of the following are your responsibilities under the NISP?

*Select all that apply.*

- ☐ Granting personnel clearances to your company’s employees
- ☐ Reviewing your company’s security procedures to ensure compliance with the NISP
- ☐ Reporting adverse security issues to the government
- ☐ Ensuring that your company’s employees protect classified documents and related information
- ☐ Educating your company’s employees on security-related issues

**Question 3**

Which of the following best describe(s) the government’s role(s) under the NISP?

*Select all that apply.*

- ☐ Establishing requirements
- ☐ Advising
- ☐ Assisting
- ☐ Overseeing
- ☐ Implementing requirements
**Question 4**

Your company has recently hired two new employees who need to obtain security clearances. Which DSS functional organization will you interact with in order to help them?

*Select the best response.*

- DSS Facility Clearance Branch
- DSS Foreign Ownership, Control, or Influence Division
- Personnel Security Management Office for Industry
- Center for the Development of Security Excellence
- DSS Counterintelligence Directorate
- Office of the Designated Approving Authority

**Question 5**

The Information System Security Manager at your company has asked you for help with your classified information system. Which DSS functional organization will be able to help you?

*Select the best response.*

- DSS Facility Clearance Branch
- DSS Foreign Ownership, Control, or Influence Division
- Personnel Security Management Office for Industry
- Center for the Development of Security Excellence
- DSS Counterintelligence Directorate
- Office of the Designated Approving Authority
**Question 6**

Which of the following are Cognizant Security Agencies in the NISP?

*Select all that apply.*

- Director of National Intelligence (DNI)
- Defense Security Service (DSS)
- Department of Energy (DOE)
- Nuclear Regulatory Commission (NRC)
- Department of Homeland Security (DHS)
- Information Security Oversight Office (ISOO)
- Department of Defense (DoD)

**Question 7**

Which of the following is the Cognizant Security Office (CSO) for the Department of Defense?

*Select the best response.*

- Office of Personnel Management
- Directorate of Defense Trade Controls
- DoD Consolidated Adjudication Facility
- Defense Security Service
Learning Activity

This activity, and others like it throughout this course, are different from standard question and answer activities. These are Learning Activities, designed to get you to explore some information or a resource to find the answers to a question. Their purpose is to teach, not to review material covered earlier, and they often serve as springboards to the presentation of new information that appears after you answer the question(s).

*Review each agency’s mission in the chart below. For each Activity below, read each scenario and question. Select the answer(s) to the questions. When you are finished, see the Learning Activity Answer Key at the end of this Student Guide to check your answers.*

<table>
<thead>
<tr>
<th>Government Agency</th>
<th>Mission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the National Counterintelligence Executive (ONCIX)</td>
<td>Protects the U.S. intelligence community and thwarts adversarial intelligence directed against U.S. interests</td>
</tr>
<tr>
<td>Central Intelligence Agency (CIA)</td>
<td>Provides national security intelligence</td>
</tr>
<tr>
<td>Defense Threat Reduction Agency (DTRA)</td>
<td>Safeguards the U.S. from weapons of mass destruction (chemical, biological, radiological, nuclear, and high yield explosives)</td>
</tr>
<tr>
<td>Interagency OPSEC Support Staff (IOSS)</td>
<td>Helps government organizations and government contractors develop operations security (OPSEC) programs</td>
</tr>
<tr>
<td>Federal Bureau of Investigation (FBI)</td>
<td>Helps protect U.S. communities and businesses from terrorism and espionage</td>
</tr>
<tr>
<td>Transportation Security Administration (TSA)</td>
<td>Protects U.S. transportation systems</td>
</tr>
<tr>
<td>State Department</td>
<td>Promotes democracy in the international community</td>
</tr>
<tr>
<td>Directorate of Defense Trade Controls (DDTC)</td>
<td>Controls the export and temporary import of defense articles and defense services covered by the United States Munitions List (USML)</td>
</tr>
<tr>
<td>DSS</td>
<td>Provides support for the National Industrial Security Program (NISP) and Security Education, Training, and Awareness (SETA).</td>
</tr>
</tbody>
</table>
Learning Activity 1: Briefings

Scenario: You are preparing a counterintelligence/threat awareness briefing for a senior manager of your company, who is planning to attend a conference in San Diego.

Which government agencies' websites are likely to provide useful information for your briefing?

Select all that apply.

- Office of the National Counterintelligence Executive (ONCIX)
- Central Intelligence Agency (CIA)
- Defense Threat Reduction Agency (DTRA)
- Interagency OPSEC Support Staff (IOSS)
- Federal Bureau of Investigation (FBI)
- Transportation Security Administration (TSA)
- State Department
- Directorate of Defense Trade Controls (DDTC)

Learning Activity 2: Briefings

Scenario: The president of your company is preparing to meet some important government officials in a country that she has never visited before. She asks you for some information about the country and its leaders.

Which government agencies' websites are likely to provide useful information for your briefing?

Select all that apply.

- Office of the National Counterintelligence Executive (ONCIX)
- Central Intelligence Agency (CIA)
- Defense Threat Reduction Agency (DTRA)
- Interagency OPSEC Support Staff (IOSS)
- Federal Bureau of Investigation (FBI)
- Transportation Security Administration (TSA)
- State Department
- Directorate of Defense Trade Controls (DDTC)
**Learning Activity 3: Operations Security**

Scenario: Your company has signed a new contract that requires additional operations security.

Which government agencies' websites are likely to provide useful information for your briefing?

*Select all that apply.*

- Office of the National Counterintelligence Executive (ONCIX)
- Central Intelligence Agency (CIA)
- Defense Threat Reduction Agency (DTRA)
- Interagency OPSEC Support Staff (IOSS)
- Federal Bureau of Investigation (FBI)
- Transportation Security Administration (TSA)
- State Department
- Directorate of Defense Trade Controls (DDTC)

**Lesson Conclusion**

In this lesson, you learned about the purpose of the NISP. You learned about your roles as an FSO in the NISP. You learned about government roles and responsibilities in the NISP, including the functions of the DSS. You also learned about a number of people, organizations, and government agency websites that you can use as resources.
Answer Key

Question 1
The purpose of the National Industrial Security Program (NISP) is to safeguard classified information in industry.

Question 2
The FSO is responsible for all of these except granting personnel clearances. Only the government can grant a clearance. The FSO’s role in personnel clearances is to help company personnel through the clearance process.

Question 3
The government is responsible for all of these except implementing requirements. That is industry’s responsibility.

Question 4
You will use the Joint Personnel Access System (JPAS) to communicate with the Personnel Security Management Office for Industry (PSMO-I) when you are helping employees obtain a personnel clearance.

Question 5
The Office of Designated Approving Authority (ODAA) facilitates certification and accreditation of classified information systems. Your IS Rep will coordinate your company’s interactions with the ODAA.

Question 6
There are four Cognizant Security Agencies (CSAs): the Director of National Intelligence (DNI), the Department of Energy (DOE), the Nuclear Regulatory Commission (NRC), and the Department of Defense (DoD).

Question 7
The DSS is the CSO that administers the NISP on behalf of the DoD and 25 other federal agencies.
Learning Activity 1: Briefings

The Office of the National Counterintelligence Executive (ONCIX) can provide counterintelligence information, the FBI website is a great source for threat awareness material, the Transportation Security Agency (TSA) website is likely to have useful information for domestic business travelers, and DSS provides security related news and alerts. Don’t forget that you can also ask your IS Rep for information from the DSS CI Directorate/Field CI Specialist.

Learning Activity 2: Briefings

The government agencies whose websites are most likely to provide information useful for an international traveler are the CIA and State Department. The CIA website includes information about international leaders and The World Factbook. The State Department website includes useful regional background information.

Learning Activity 3: Operations Security

The Interagency OPSEC Support Staff (IOSS) is responsible for helping government organizations develop their own operations security (OPSEC) programs.
Lesson Introduction

The government provides several important documents to help you comply with the requirements of the National Industrial Security Program (NISP). Your primary reference will be the National Industrial Security Program Operating Manual (NISPOM) which provides the baseline security requirements for protecting classified information within the U.S. government contractor community.

In this lesson, you will learn how the NISPOM is organized, and how to find NISP requirements for different types of secure facilities. You will also learn what types of events you must report to the government and how to report them.

The lesson objectives are to be able to:

- Identify the structure of the National Industrial Security Program Operating Manual (NISPOM)
- Identify the purpose of and how to access Industrial Security Letters (ISLs) and the NISPOM index
- Identify NISPOM requirements that apply to different types of facilities
- Identify NISPOM reporting requirements

NISP Policy Documents

**Sponsorship in the NISP**

Several important documents will guide your company’s participation in the NISP. You will understand the purpose of each of these documents if you remember the context in which your company receives them.

Let’s start with how a company becomes part of the NISP. To join the 13,000 plus contractors that are already involved in the NISP, a company must be sponsored. There are two ways to be sponsored into the NISP. The contracting office of a government agency, known as a Government Contracting Activity (GCA) may
sponsor a company when the GCA wants to do business with that company and the business requires access to classified information. Or, a company that is already part of the program may sponsor a company in order to sub-contract part of its classified business.

To sponsor a company, the GCA or prime contractor puts in a request, called a sponsorship letter, to the appropriate Cognizant Security Agency (CSA), for example, the Department of Defense (DoD). When the CSA is the DoD, the letter goes to the Defense Security Service (DSS) which functions as the Cognizant Security Office (CSO) on behalf of the DoD.

**General NISP Guidance**

When your company becomes part of the NISP, the contractual relationship between the government and your company is codified in the DD Form 441, Department of Defense Security Agreement. This form is a legally binding contract between your company and the U.S. government. Attached to the DD Form 441, and part of the contract, is DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM). The NISPOM is a compilation of security requirements based on federal statutes, directives, and executive orders.

By signing the DD Form 441, your company agrees to maintain security controls and procedures in accordance with the NISPOM. The DD Form 441 indicates that your company has become part of the NISP. It is not a contract for specific work with the government.

**Contract-Specific Guidance**

Once a company becomes part of the NISP, the GCA can issue a contract that requires the company to have access to classified information. The GCA attaches the DD Form 254, Department of Defense Contract Security Classification Specification, to all such contracts.

This form provides contract-specific guidance about what information is classified and at which level. It may include specific security requirements that go beyond the overall policy guidance provided by the NISPOM. Special Access Program (SAP) contracts will also include enhanced security requirements found in the NISPOM Supplement. Even though the DD Form 254 is contract-specific, it is not all-inclusive. Additional security requirements are sometimes included in other parts of a contract. As an FSO, you may sometimes need additional guidance or clarification from the GCA.
The NISPOM

The FSO and the NISPOM

As a Facility Security Officer (FSO), you are responsible for ensuring that your company complies with guidance in the NISPOM. You will need to determine which NISPOM requirements apply to your company, and then ensure that they are implemented by conveying them to everyone in your company. The NISPOM is performance-based; it provides requirements but not procedures for how to fulfill them. It is your job to determine how to implement the requirements in the NISPOM. Your Industrial Security Representative (IS Rep) can assist you if you have questions regarding NISPOM requirements at your facility. You may find that it is helpful to convey and implement NISPOM requirements through written Standard Practice Procedures (SPPs). Talk with your IS Rep about whether this is a good approach at your facility.

Information for All FSOs

Let’s look at what kind of information is in the NISPOM. The NISPOM spells out the acronyms associated with the NISP. It has eleven chapters and several appendices, including a glossary of terms.

Which parts of the NISPOM apply to your facility? Chapters 1, 2, 3, and 6 apply to all NISP contractors, and all NISP contractors should be familiar with the information in Appendices A and C. In addition, every FSO should have a working knowledge of the sections of Chapter 5 that cover safeguarding oral discussions and the disclosure of classified information. You should familiarize yourself with these parts of the NISPOM. Review each highlighted section of the Table of Contents to see a brief description of its contents and how it relates to your FSO roles in the chart on the next page.
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>NISPM Chapter</th>
<th>How the Chapter Relates to Your FSO Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS</td>
<td>• Provides an overview of the NISP, including general requirements and reporting requirements for facilities participating in the NISP</td>
</tr>
<tr>
<td>CHAPTER 2. SECURITY CLEARANCES</td>
<td>• Provides information about facility clearances for facilities participating in the NISP and personnel security clearances for employees of and consultants to those facilities</td>
</tr>
<tr>
<td></td>
<td>• Addresses foreign ownership, control or influence (FOCI) of facilities in Section 3</td>
</tr>
<tr>
<td>CHAPTER 3. SECURITY TRAINING AND BRIEFINGS</td>
<td>• Provides the basic requirements for training of the FSO and cleared employees of a facility participating in the NISP</td>
</tr>
<tr>
<td>CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION</td>
<td>• States provisions for protection of classified information and material</td>
</tr>
<tr>
<td>CHAPTER 6. VISITS AND MEETINGS</td>
<td>• Provides requirements for classified visits and classified meetings</td>
</tr>
<tr>
<td>Appendix A. Cognizant Security Office Information</td>
<td>• Lists contact information for the CSOs for the four CSAs under the NISP</td>
</tr>
</tbody>
</table>

### Acronyms

- CSO: Cognizant Security Office
- CSA: Category System Advisor
- NISP: National Industrial Security Program
- RFV: Request for Visit Format
### NISPOM Chapter | How the Chapter Relates to Your FSO Roles
---|---
Appendix C. Definitions | - Provides an alphabetical list of key industrial security definitions -- some terms and phrases have a unique meaning in the context of the NISP

### Learning Activity 1: Specialized Information

This activity, and others like it throughout this course, are different from standard question and answer activities. These are Learning Activities, designed to get you to explore some information or a resource to find the answers to a question. Their purpose is to teach, not to review material covered earlier, and they often serve as springboards to the presentation of new information that appears after you answer the question(s).

When you are finished with each activity, see the Learning Activity Answer Key at the end of this Student Guide to check your answers.

The other chapters in the NISPOM may or may not apply to you. To find out which sections apply, answer the questions below. If you are not sure, answer, “I don’t know.” You will need to find out later and then familiarize yourself with the appropriate sections of the NISPOM.

---

### TABLE OF CONTENTS

**Acronyms**

- CHAPTER 1. GENERAL PROVISIONS AND REQUIREMENTS
- CHAPTER 2. SECURITY CLEARANCES
- CHAPTER 3. SECURITY TRAINING AND BRIEFINGS
- CHAPTER 4. CLASSIFICATION AND MARKING
- CHAPTER 5. SAFEGUARDING CLASSIFIED INFORMATION
- CHAPTER 6. VISITS and MEETINGS
- CHAPTER 7. SUBCONTRACTING
- CHAPTER 8. INFORMATION SYSTEM SECURITY
- CHAPTER 9. SPECIAL REQUIREMENTS
- CHAPTER 10. INTERNATIONAL SECURITY REQUIREMENTS
- CHAPTER 11. MISCELLANEOUS INFORMATION

**APPENDICES**

- Appendix A. Cognizant Security Office Information
- Appendix B. International Visits Standard Request for Visit Format (RFV)
- Appendix C. Definitions
**Question 1**

Does your facility generate classified materials?

- Yes
- No
- I don’t know

*If your facility generates classified materials, then you need to have a working knowledge of the information in Chapter 4, Classification and Marking. This chapter provides an overview of the classification system and requirements for classified material to be properly marked.*

**Question 2**

Has your facility been approved to maintain possession of classified materials?

- Yes
- No
- I don’t know

*If your facility stores classified materials, then you must have a working knowledge of all of Chapter 5, Safeguarding Classified Information.*

**Question 3**

Is your company a prime contractor with classified sub-contracts?

- Yes
- No
- I don’t know

*If your company is a prime contractor with classified sub-contracts, then you must have a working knowledge of the requirements for classified sub-contracts in Chapter 7, Subcontracting.*
**Question 4**

Is your company a sub-contractor on classified contracts?

- Yes
- No
- I don’t know

*If your company works as a sub-contractor on classified contracts, then you must have a working knowledge of the requirements for classified sub-contracts in Chapter 7, Subcontracting.*

**Question 5**

Does your company have a classified information system or does it intend to process classified information on an information system in the future?

- Yes
- No
- I don’t know

*If your facility has a classified information system or intends to process classified information in the future, you should understand the requirements in Chapter 8, Information System Security.*

**Question 6**

Does your company have contracts that involve any of the following types of information?

- Restricted Data (RD)
- Formerly Restricted Data (FRD)
- Critical Nuclear Weapon Design Information (CNWDI)
- Intelligence information
- Communications Security (COMSEC) information

- Yes
- No
- I don’t know
If your company has contracts that involve any of these types of information, then you should familiarize yourself with the appropriate sections of Chapter 9, Special Requirements.

Question 7
Do your company’s employees have access to foreign government information (FGI) or to information that is classified by the North Atlantic Treaty Organization (NATO)?

- Yes
- No
- I don’t know

International security requirements in Chapter 10 may apply if your company’s employees have access to classified FGI or to NATO classified information. If so, then you should familiarize yourself with the appropriate sections.

Question 8
Is anyone at your facility involved in any way with the disclosure of classified information to a foreign entity, with receipt of classified information from a foreign entity, or with classified visits to or from a foreign entity?

- Yes
- No
- I don’t know

Parts of Chapter 10 may apply if your facility is involved with foreign entities in these ways.

Question 9
Does your facility have contracts that include TEMPEST requirements?

- Yes
- No
- I don’t know

If your facility has contracts containing TEMPEST requirements, then you must have a working knowledge of the information in Chapter 11, Section 1.
Question 10

Does your company use or would it like to use the services of the Defense Technical Information Center (DTIC)?

- Yes
- No
- I don’t know

DTIC is the central point within the DoD for acquiring, storing, retrieving, and disseminating scientific and technical information to support the management and conduct of DoD research, development, testing, and evaluation (RDT&E) programs. If your company uses or would like to use DTIC services, then you must have a working knowledge of the information in Chapter 11, Section 2.

Question 11

Is your company involved in independent research and development (IR&D) efforts that involve classified information?

- Yes
- No
- I don’t know

If your company is involved in classified IR&D efforts, then you must have a working knowledge of the provisions of Chapter 11, Section 3.

Question 12

Does your company send employees on classified international visits?

- Yes
- No
- I don’t know

Appendix B: covers the procedures for sending cleared employees on international visits.
Structure and Organization

Now let’s look more closely at how the NISPOM is structured.

Each chapter in the NISPOM is divided into sections, which are shown in the Table of Contents. There are three sections in Chapter 1. Each section is further divided into paragraphs. You can find your way around the NISPOM if you understand how the paragraphs and pages are numbered.

Each paragraph number has three components. The first component, before the dash, is the chapter number. The number immediately after the dash is the section number, which is followed by the two-digit paragraph number. In this example, paragraph number 1-205 is called Security Training and Briefings. Notice that the first paragraph in each section is paragraph 00.

Page numbers in the NISPOM also have three parts. The first number is the chapter number, the second number is the section number, and the last number is the page number within that section.
Note in the Table of Contents that paragraph 1-205, Security Training and Briefings, starts on page 1-2-1, which is the first page of the second section of Chapter 1.

Let's look at that page.

Here you can see paragraph 1-205 on page 1-2-1.

Now look at paragraph 1-206. Sometimes a paragraph number refers to more than one physical paragraph. When this is the case, the sub-paragraphs will be lettered and sub-sub-paragraphs will be numbered, as you see here. You will have an opportunity to practice using the NISPOM in a few moments, but first let's look at some additional NISPOM-related materials that are available.
**Index and ISLs**

As you have seen, the NISPOM is organized hierarchically. Soon you will be familiar with the chapters you use most, and you will be able to find the information you need quickly. But what if you wanted to look up something very specific and were not sure what chapter to look in? In that case, you might want to use the NISPOM Index. The NISPOM Index is not in the NISPOM. It is a separate document available online. You may want to print the NISPOM index and keep it with your copy of the NISPOM.

Sometimes the government needs to change or clarify national industrial security policies or requirements. To keep you up-to-date on the latest developments in industrial security, the DSS publishes Industrial Security Letters (ISLs) and posts them on its website. Since ISLs are published as needed, it’s a good security practice to check for updates regularly.

**Review Activity 1: The NISPOM**

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.
**Situation 1**

A company employee asks for assistance in applying for a personnel security clearance.

*Look in the NISPOM Table of Contents. Then select the chapter that provides the guidance you need to help this employee.*

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4

**Situation 2**

Your Information System Security Manager (ISSM) has a question about his responsibilities on your company’s classified information system.

*Look in the NISPOM Table of Contents. Then select the chapter that provides the guidance you need to help this employee.*

- Chapter 2
- Chapter 4
- Chapter 6
- Chapter 8

**Situation 3**

You are not sure how to store a large volume of classified documents.

*Look in the NISPOM Table of Contents. Then select the chapter that provides the guidance you need.*

- Chapter 1
- Chapter 3
- Chapter 5
- Chapter 7
Situation 4

Which of these numbers is a NISPOM page number and which is a paragraph number?

Match the description on the left to the appropriate number on the right.

Page number 10-509
Paragraph number 9-4-2

Situation 5

What is an Industrial Security Letter (ISL)?

Select the best answer.

○ A request to admit a company into the National Industrial Security Program
○ A document that provides changes or clarification to national industrial security policy requirements
○ A document that codifies a company’s relationship with the government when that company joins the NISP
○ A document that specifies what information is classified for a particular contract

Situation 6

Where can you find the NISPOM Index?

Select the best answer.

○ Before Chapter 1 in the NISPOM
○ After the last Appendix in the NISPOM
○ In the NISPOM Supplement
○ None of the above
Reporting Requirements

*Introduction to NISP Reporting*

One of your roles as an FSO is to report certain types of events or information to the appropriate government agencies. In the following activity, you will learn what you are required to report and to whom. You will also gain valuable experience finding information in the NISPOM, which will be available to help you throughout the activity. You will learn more about reporting requirements in another course in this curriculum.

*Learning Activity 2: Find Reporting Requirements*

Read the question and find the answer in the NISPOM. Where in the NISPOM will you find FSO reporting requirements?

*Select the best answer.*

- Chapter 1, Section 3
- Chapter 3, Section 1
- Chapter 4, Section 2
- Chapter 2, Section 4

*Learning Activity 3: What to Report*

Read the question and find the answer in the identified paragraph of the NISPOM. According to NISPOM paragraph 1-300, which of the following are you required to report to the government?

*Select the best answer.*

- The number of classified documents stored in your facility
- The number of cleared personnel working in your facility
- Events that affect the status of an employee’s personnel security clearance
- Events that require the facility to be open during non-business hours
**Learning Activity 4: Where to Report**

Read the question, and find the answer by consulting the identified paragraphs of the NISPOM. According to NISPOM paragraphs 1-301 and 1-302, to which government agencies are you required to report the events listed in paragraph 1-300?

*Select all that apply.*

- Federal Bureau of Investigation (FBI)
- Department of Homeland Security (DHS)
- Information Security Oversight Office (ISOO)
- Cognizant Security Agency (CSA)

**Learning Activity 5: FBI Reports**

According to NISPOM paragraphs 1-301, you must report actual, probable, or possible espionage, sabotage, terrorism, or subversive activities to the FBI. Which of these situations do you think you should report to the FBI along with a copy to your CSA?

*Select all that apply.*

- You have inconclusive evidence that an employee may have sold Confidential materials to alleviate his financial stress.
- A cleared employee just married a foreigner.
- A cleared employee is planning a vacation to Israel.
- A safe containing classified information appears to have been tampered with.
- There was a small explosion in your classified facility’s boiler room. No materials were compromised. It’s not clear what caused the explosion but circumstances cause you to suspect that someone may have set off the explosion.
Reporting to the FBI

If you suspect or know of espionage, sabotage, terrorism or subversive activities each of which are explained in the chart below, you must report it to the nearest FBI field office. If the matter is urgent, you may file your initial report over the phone, but you must then follow up with a written report. The NISPOM requires that you file a copy of your FBI report with your CSA. This copy should be sent to your IS Rep. Do not act without guidance from the FBI!

The FBI will investigate and determine what, if any, further action is appropriate. They may also refer the situation to another government agency.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Espionage</td>
<td>The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.</td>
</tr>
<tr>
<td>Sabotage</td>
<td>An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war materiel, premises, or utilities, to include human and natural resources.</td>
</tr>
<tr>
<td>Terrorism</td>
<td>The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.</td>
</tr>
<tr>
<td>Subversive Activities</td>
<td>Anyone lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of incumbent governments by force and violence is subversive and is engaged in subversive activity. All willful acts that are intended to be detrimental to the best interests of the government and that do not fall into the categories of treason, sedition, sabotage, or espionage will be placed in the category of subversive activity.</td>
</tr>
</tbody>
</table>
Reporting to the CSA

Now let’s consider what you must report to the CSA. In general, you must report to the CSA anything that might affect the personnel security clearances of any of your company’s employees, or anything that might affect your facility clearance, including your facility’s ability to protect classified materials. The NISPOM specifies what you must report to the CSA, but since each CSA handles these reporting requirements differently, the NISPOM does not specify how to report to the CSA.

When the DoD is your CSA, you will send CSA reports to DSS. As the CSO, DSS receives the reports and acts on behalf of DoD, the CSA. In general, you will send reports about personnel security clearances to the Personnel Security Management Office for Industry (PSMO-I). You will send reports about your facility clearance and other issues to your IS Rep.

Learning Activity 6: Personnel Security Management Office for Industry (PSMO-I) Reports

NISPOM paragraph 1-302 has sub paragraphs that list 14 different types of information and events that you must report to the CSA. The first seven are shown here. Which of these cover events or information that you should report to the PSMO-I?

Select all that apply.

☐ 1-302 a: Adverse Information (about a cleared employee)
☐ 1-302 b: Suspicious Contacts
☐ 1-302 c: Change in Cleared Employee Status
☐ 1-302 d: Citizenship by Naturalization (for an employee with access to classified information)
☐ 1-302 e: Employees Desiring Not to Perform on Classified Work
☐ 1-302 f: Standard Form (SF) 312 (employee refusal to execute the Classified Information Nondisclosure Agreement)
☐ 1-302 g: Change Conditions Affecting the Facility Clearance
**Reporting to Personnel Security Management Office for Industry (PSMO-I)**

Here again are the five types of information or events from NISPOM paragraph 1-302 that you should report to the PSMO-I:

- Adverse Information
- Changes in Cleared Employee Status
- Citizenship by Naturalization
- Employees Desiring Not to Perform on Classified Work
- Standard Form (SF) 312

You report all of these events to the PSMO-I through the Joint Personnel Adjudication System (JPAS). You may also provide these reports directly to the PSMO-I in writing.

Review each type of information or event below to learn more.

**Adverse Information**

If you receive credible adverse information about a cleared employee at your facility, you must report it to the PSMO-I through the incident report feature of JPAS. Adverse information is employee behavior that might cause the DoD to question whether that employee should have access to classified information. To understand the type of information you should report, familiarize yourself with the DoD’s Adjudicative Guidelines for Determining Eligibility for Access to Classified Information. Remember, however, that your job is to report credible adverse information. The decision about whether to grant or continue a personnel security clearance is the government’s, not yours. DoD adjudicative guidelines include discussions of each of the following categories:

- Allegiance to the United States
- Foreign influence
- Foreign preference
- Sexual behavior
- Personal conduct
- Financial considerations
- Alcohol consumption
- Drug involvement
- Emotional, mental, and personality disorders
- Criminal conduct
- Security violations
- Outside activities
- Misuse of information technology systems

**Changes in Cleared Employee Status**

You must report certain changes in the status of cleared employees to the PSMO-I through JPAS. These include:

- Death
- Name change
- Employment termination
- Citizenship change in status
- End of access to classified information, such as when the employee is assigned a new job where he or she no longer needs access

**Citizenship by Naturalization**

If a non-U.S. citizen who has been granted limited access to classified information in your facility becomes a U.S. citizen, you must report details about that employee’s naturalization to the PSMO-I through JPAS. The details you must report include:

- City, county, state where the employee became a citizen
- Date when the employee became a citizen
- Court that granted citizenship
- Employee’s naturalization certificate number

**Employees Desiring Not to Perform on Classified Work**

If an employee at your facility expresses a desire not to perform classified work, you must report that to the PSMO-I through the Joint Personnel Access System (JPAS). This applies to employees who are being processed for a clearance and decide to discontinue the clearance process, and to employees who already hold clearances and would like to relinquish them.
Refusal to Execute SF 312

If any cleared employee refuses to complete and sign Standard Form (SF) 312, Classified Information Nondisclosure Agreement, you must report that to the PSMO-I through JPAS. This form is a required part of the personnel clearance process.

Reporting Individual Culpability

In addition to the information and event types listed in NISPOM paragraph 1-302, you must also use JPAS to report individual culpability to the PSMO-I. Individual culpability is covered in paragraph 1-304. Go to the NISPOM and read that paragraph. Then try the exercise that follows.

Learning Activity 7: Individual Culpability Reports

According to NISPOM paragraph 1-304, which of the following cleared employees do you think you should report to the PSMO-I?

Select all that apply.

- □ Jack took classified work home with him over the weekend. He knew it was a security violation, but he was trying to meet a deadline. This was his first violation.
- □ Mary puts the wrong classification markings on her reports even though she has been instructed repeatedly on proper marking procedures.
- □ Vera accidentally left a classified file out when she went to lunch and the only person in the area was a cleared employee. This was her first violation.
- □ Tom is usually very careful, but one night he finished working with a Secret document after the security container had been closed. He didn’t know the combination, so he locked the document in his desk drawer instead of finding someone who could put it in the appropriate container.

Reporting to the IS Rep

Of the 14 sub-paragraphs listed in NISPOM paragraph 1-302, you have seen that five describe information and events that you must report to the PSMO-I. The information and events listed in all of the remaining sub-paragraphs must be reported to your IS Rep.
Review each type of information or event below to learn more.

<table>
<thead>
<tr>
<th>Type of Information or Event</th>
<th>Report to IS Rep</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-302 b. Suspicious Contacts</td>
<td>• Attempts to gain unauthorized access to classified information</td>
</tr>
<tr>
<td></td>
<td>• Attempts to compromise a cleared employee</td>
</tr>
<tr>
<td></td>
<td>• Contacts between cleared employees and foreign intelligence officers</td>
</tr>
<tr>
<td>1-302 g. Change Conditions Affecting the Facility Clearance</td>
<td>• Report changes in:</td>
</tr>
<tr>
<td></td>
<td>o Company name</td>
</tr>
<tr>
<td></td>
<td>o Company or cleared facility address</td>
</tr>
<tr>
<td></td>
<td>o Key management personnel (KMP)</td>
</tr>
<tr>
<td></td>
<td>o Foreign ownership, control, or influence (FOCI)</td>
</tr>
<tr>
<td></td>
<td>• Report termination of company operations, including bankruptcy proceedings</td>
</tr>
<tr>
<td>1-302 h. Changes in Storage Capability</td>
<td>Report any changes that might increase or decrease the amount of classified material your facility is approved to protect</td>
</tr>
<tr>
<td>1-302 i. Inability to Safeguard Classified Material</td>
<td>Report emergency situations that make your facility incapable of safeguarding classified information</td>
</tr>
<tr>
<td>1-302 j. Security Equipment Vulnerabilities</td>
<td>Report vulnerabilities in:</td>
</tr>
<tr>
<td></td>
<td>• Hardware</td>
</tr>
<tr>
<td></td>
<td>• Software</td>
</tr>
<tr>
<td></td>
<td>• Security systems</td>
</tr>
<tr>
<td>1-302 k. Unauthorized Receipt of Classified Material</td>
<td>Report receipt or discovery of classified material that your facility is not authorized to have.</td>
</tr>
<tr>
<td>1-302 l. Employee Information in Compromise Cases</td>
<td>NISPOM paragraph 1-303 covers procedures for reporting the loss, compromise, or suspected compromise of classified materials.</td>
</tr>
<tr>
<td>1-302 m. Disposition of Classified Material Terminated From Accountability</td>
<td>Report discovery of classified material that was previously reported as lost.</td>
</tr>
<tr>
<td>1-302 n. Foreign Classified Contracts</td>
<td>Report negotiations that could involve:</td>
</tr>
<tr>
<td></td>
<td>• Release of U.S. classified information to a foreign interest</td>
</tr>
<tr>
<td></td>
<td>• Access to foreign classified information</td>
</tr>
</tbody>
</table>
Learning Activity 8: Facility Clearance Changes

According to NISPOM paragraph 1-302 g, which of the following do you think you should report as a changed condition that might affect your facility clearance?

Select your best answer.

- Twelve new employees were hired and require personnel clearances.
- Your company has changed its name.
- Your facility is expanding.
- A member of your staff was arrested for possession of a firearm.

Learning Activity 9: IS Rep Reports

Which of the following situations do you think you should report to your IS Rep?

Review NISPOM 1-302, if you wish, and select all that apply.

- Situation 1: An uncleared friend is asking questions about classified projects your employees work on.
- Situation 2: An employee received Top Secret documents from a DoD employee. Your facility is cleared to the Secret level.
- Situation 3: The president of your company is in pre-contract negotiations with a British company that may lead to the disclosure of U.S. classified information.
- Situation 4: Your alarm system has been malfunctioning.
Review Activity 2: Reporting Requirements

How should you report these events?

_Read each scenario and decide to which person or organization you should report each scenario. Write the letter of the corresponding person or organization next to each scenario._

Mark left a classified document out overnight. Uncleared janitors were in the area.

- [ ] a. FBI
- [ ] b. PSMO-I
- [ ] c. IS Rep

Pam O’Brien got married and changed her name to Pam Nemirovsky.

Pat tells a co-worker that he plans to sell classified information to a Foreign Intelligence Service.

Sara received a request for classified information from an uncleared person she met at a conference.

Your company purchased its first GSA-approved container, enabling it to now store Secret material in addition to Confidential material it presently possesses.
Lesson Conclusion

In this lesson, you learned about the NISPOM, including how it is organized and which chapters apply to which kinds of facilities. You also learned about ISLs and the NISPOM index. And you learned about the events and information you are required to report to the government under the NISP.

Review the types of events you should report to each entity:

<table>
<thead>
<tr>
<th>Report to</th>
<th>Event Type</th>
</tr>
</thead>
</table>
| FBI       | • Espionage  
               • Sabotage  
               • Terrorism  
               • Subversive actions |
| IS Rep    | • Suspicious contacts  
               • Changes that affect facility clearance  
               • Changes in storage capability  
               • Emergency inability to safeguard classified material  
               • Security equipment vulnerabilities  
               • Unauthorized receipt of classified material  
               • Disposition of material terminated from accountability  
               • Loss, compromise, suspected compromise  
               • Possible involvement in foreign classified contracts |
| PSMO-I    | • Adverse information  
               • Change in employee status  
               • Citizenship by naturalization  
               • Employees desiring not to perform on classified work  
               • Employee refusal to execute SF 312  
               • Individual culpability actions |
Answer Key

*Review Activity 1: The NISPOM*

**Situation 1**
*Chapter 2, Security Clearances*, provides information about facility clearances and personnel clearances.

**Situation 2**
Classified information system security requirements, including the ISSM’s responsibilities, are in *Chapter 8, Information System Security*.

**Situation 3**
*Chapter 5, Safeguarding Classified Information*, covers storage and storage equipment for classified materials.

**Situation 4**
*Paragraph number 10-509* is in Chapter 10, Section 5. *Page number 9-4-2* is the second page in Chapter 9, Section 4.

**Situation 5**
An ISL is issued by the DSS when the government *makes changes to or needs to clarify national industrial security policy requirements*. ISLs keep you up to date on the latest developments in industrial security.

**Situation 6**
*None of the above*. The NISPOM Index is a separate document that you can access through the DSS website.

*Review Activity 2: Reporting Requirements*

The correct answers are c, b, a, c, and c. Here is an explanation for each:

- Mark’s situation is a suspected compromise, which you would report to your IS Rep. If you determined that there was gross negligence, deliberate disregard for security, or a pattern of carelessness involved, you would also send an incident report through JPAS to the PSMO-I. (NISPOM 1-303, 1-304)

- Pam’s name change should be reported to the PSMO-I. (NISPOM 1-302 c)
FSO Role in the NISP
Policy Guidance and Reporting Requirements

- Pat’s situation is possible espionage, which you should report promptly to the FBI. You would send a copy of your report to your IS Rep. (NISPOM 1-301)
- Sara has received a suspicious contact, which you should report to your IS Rep. (NISPOM 1-302 b)
- The change in your company’s classified material storage capacity must also be reported to your IS Rep. (NISPOM 1-302 h)

Learning Activity 2: Finding Reporting Requirements

Chapter 1, Section 3 of the NISPOM is called Reporting Requirements.

Learning Activity 3: What to Report

According to NISPOM paragraph 1-300, you must report certain events that affect an employee’s personnel clearance. In addition, you are required to report events that affect your facility clearance status, events that affect the safeguarding of classified information, and events that indicate that classified information has been lost or compromised.

Learning Activity 4: Where to Report

Paragraph 1-301 covers reports to be submitted to the FBI and paragraph 1-302 covers reports to be submitted to the CSA. If your CSA is the DoD, you will report to the CSA via the DSS.

Learning Activity 5: FBI Reports

These situations represent actual, probable, or possible cases of espionage, sabotage, or terrorism:

- You have inconclusive evidence that an employee may have sold Confidential materials to alleviate his financial stress.
- A safe containing classified information appears to have been tampered with.
- There was a small explosion in your classified facility’s boiler room. No materials were compromised. It’s not clear what caused the explosion but circumstances cause you to suspect that someone may have set off the explosion.
Learning Activity 6: PSMO-I Reports

You report events or information related to personnel security clearances to the PSMO-I. These include:

- Adverse information about a cleared employee
- Changes in the status of a cleared employee
- Citizenship by naturalization for an employee with access to classified information
- Cleared employees who decide they no longer want to work with classified information
- Employees who refuse to execute the Classified Information Nondisclosure Agreement

Learning Activity 7: Individual Culpability Reports

You should report Jack, Mary, and Tom.

According to NISPOM paragraph 1-304, your company must establish and enforce a system of administrative actions against employees who violate security requirements. You must report these actions to the PSMO-I (via the incident report feature of JPAS) in the following circumstances:

- When the employee deliberately disregarded security requirements
- When he employee exhibited gross negligence in the handling of classified material
- When the employee has exhibited a pattern of negligence or carelessness

Here is an explanation of the correct answers:

- You should report the administrative action taken against Jack, even though this is his first violation because he deliberately disregarded the rules.
- You should also report the action taken against Mary, who has exhibited a pattern of carelessness.
- It is not necessary to report the action taken against Vera, who made one accidental mistake, with no chance of compromise.
- You should report the action taken against Tom, despite his good record, because this was an act of gross negligence.

**Learning Activity 8: Facility Clearance Changes**

According to NISPOM paragraph 1-302 g, you must report a **company name change**. You must also report the following conditions that might affect your facility clearance:

- Changes in company or cleared facility address
- Changes to key management personnel (KMP)
- Termination of company operations, including bankruptcy proceedings
- Changes in foreign ownership, control, or influence (FOCI)

**Learning Activity 9: IS Rep Reports**

Report **all of these situations**. Here is an explanation for each:

- According to NISPOM sub-paragraph 1-302 b, you should report all suspicious contacts. This includes anyone who asks for unauthorized access to classified information.
- According to NISPOM sub-paragraph 1-302 k, you should report any unauthorized receipt of classified material. If your facility is cleared to the Secret level, then your employees are not authorized to receive Top Secret material.
- According to NISPOM sub-paragraph 1-302 n, Foreign Classified Contracts, you must report the situation where the president of your company is in pre-contract negotiations with a British company that may lead to the disclosure of U.S. classified information. If you are in this situation, you should also review the international security requirements in Chapter 10 of the NISPOM.
- According to NISPOM sub-paragraph 1-302 j, you must report security equipment vulnerabilities. This includes alarm systems.
Lesson Introduction

In this lesson, you will be introduced to many of the resources that are available to help you fulfill the roles of a Facility Security Officer (FSO) in the National Industrial Security Program (NISP).

The lesson objectives are to be able to:

- Identify and access resources needed to do the following:
  - Manage security program to obtain and maintain facility clearances
  - Obtain and maintain personnel security clearances
  - Provide security education, training, and awareness
  - Properly mark, safeguard, and transmit/transport classified materials
  - Conduct industrial security self-inspections

- Identify and access the following additional resources:
  - Hotlines for reporting industrial security issues
  - Professional organizations related to industrial security

FSO Resources

Finding FSO Resources

There are many resources available to assist you in fulfilling your responsibilities as an FSO. This course contains several resources that you can access by selecting the Resources tab on the course navigation bar and visiting the Course Resources Page. This page lists regulatory documents, forms, and other tools specifically discussed in this course. CDSE also provides centralized access to many of the other relevant resources on its website under Industrial Security. In addition to
training courses, CDSE offers job aids, brochures and guides and links to outside sites that house regulatory guidance and other information for security professionals.

**FSO Resources Overview**

You have already learned about many resources and references that you may consult to help you fulfill your responsibilities as an FSO. You have also been introduced to some additional resources as you learned about each of your FSO roles.

We will look first at general resources, and then at resources that are specific to each of your roles. You are not expected to memorize all the resources, but if you are familiar with what is available, your job will be easier.

**General Resources**

Let’s look first at the resources that can help you in all your roles as an FSO. In addition to the resources you have already learned about, you may wish to join one or more professional organizations so that you can network with other FSOs and access best practices, training, and other useful resources.

Organizations for security professionals include the American Society for Industrial Security (ASIS) International; NCMS, The Society of Industrial Security Professionals; the Extranet for Security Professionals; and industrial security awareness councils. You can access some of these organizations’ websites through the CDSE website and the Course Resources page. Review each professional organization below to learn more.

**ASIS International**

ASIS International is the largest organization for security professionals with over 38,000 members worldwide. An ASIS membership includes a range of security programs and services and a subscription to Security Management.

**NCMS**

NCMS is the Society of Industrial Security Professionals. This organization has over 5,000 members representing federal agencies, civilian contractors, and foreign countries. By joining NCMS, you can take advantage of professional
development opportunities in many security-related disciplines such as the following:

- Facility security
- Personnel security
- Classification management
- Information security
- Computer security
- Technology security
- Operations security

Look on the NCMS website for a chapter near you.

Extranet for Security Professionals

The Extranet for Security Professionals is a secure online environment offered by the OPM Center for Federal Investigative Services. You can use this secure portal to conduct research and collaborate with other security professionals; however, you should not use the portal for classified discussions.

Industrial Security Awareness Councils (ISACs)

Industrial security awareness councils (ISACs) are informal, geographically-organized, non-profit associations of defense contractors, government agencies, and the DSS. ISACs promote security awareness in the defense industry by focusing the collective energy and resources of industry and government. Check with your Industrial Security Representative (IS Rep) to find out more information about your local ISAC.
### Previous Resources: General FSO Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DD Form 441, DoD Security Agreement</td>
<td>A general agreement between the DoD and a contractor who will have access to classified information</td>
</tr>
<tr>
<td>DD Form 254, DoD Contract Security Classification Specification</td>
<td>Contract-specific guidance about what information is classified and at which level</td>
</tr>
<tr>
<td>Center for Development of Security Excellence (CDSE)</td>
<td>Provides security education and training to DoD and other U.S. government personnel and contractors</td>
</tr>
<tr>
<td>Facility Security Officer (FSO)</td>
<td>Contractor-appointed employee who supervises and directs security measures necessary for implementing the NISPOM</td>
</tr>
<tr>
<td>Industrial Security Representative (IS Rep)</td>
<td>Represents DSS for security matters covered by the NISP</td>
</tr>
<tr>
<td>Industrial Security Letter (ISL)</td>
<td>Detailed operational guidance and notification of changes to or clarification of existing policy requirements in the NISPOM</td>
</tr>
<tr>
<td>National Industrial Security Program Operating Manual (NISPOM)</td>
<td>Prescribes requirements, restrictions, and safeguards to prevent unauthorized disclosure of classified information in industry</td>
</tr>
</tbody>
</table>

### Facility Clearance Resources

Now let’s look at the resources you are likely to use as you manage your security program in order to obtain and maintain your facility clearance. Some that you have already seen are the IS Rep, the NISPOM, the DSS Facility Clearance Branch, the DSS FOCI Operations Division, the Center for Development of Security Excellence, and the Facility Clearances in the NISP Course.

In addition to these resources, you might find the Facility Clearance Checklist helpful. You will need to know how to use the Industrial Security Facilities Database (ISFD), Electronic Facility Clearance System (e-FCL), and if your company subcontracts any of its classified work, you will need the Guide for Preparation of the DD Form 254. Review each of these additional resources below to learn more.
Facility Clearance Checklist

The Facility Clearance Checklist includes all the steps that are necessary for processing a facility clearance, and a list of the documents and information you must gather in preparation for your IS Rep’s first visit to your facility. You should print this checklist and check off each item as it is completed.

Industrial Security Facilities Database (ISFD)

The ISFD is the DoD system for facility clearance information. Once your facility has been granted an interim facility clearance, you can use this system to check on the status. You might find the ISFD Facility Clearance Verification and Notification for Industry Course helpful.

DD Form 254 Handbook

As you know, when the government contracts with your company under the NISP, the GCA attaches a DD Form 254 to the contract. This form provides contract-specific guidance about what information is classified and at which level. Personnel at the GCA might use the Guide for the Preparation of a DD Form 254 to complete this form. If your company decides to subcontract some of its classified work, then you will be required, as a prime contractor, to prepare a DD Form 254 for the subcontracting company. You can use the step-by-step procedures in the Guide for Preparation of a DD Form 254 to assist you when completing the form for your subcontractor.

e-FCL

Use of the Electronic Facility Clearance System (e-FCL) is required for all companies in process for a facility clearance or reporting a changed condition. The web-based e-FCL is designed around the SF-328, Certificate Pertaining to Foreign Interests, and allows companies to upload and submit their facility information into the system. This information includes the SF 328 itself, key management personnel list, stockholders list, articles of incorporation, corporate bylaws, and other supporting documents. Companies operating under a FOCI mitigation agreement must use e-FCL for annual certification processing.
## Previous Resources: Facility Clearance Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Security Representative (IS Rep)</td>
<td>Represents DSS for security matters covered by the NISP</td>
</tr>
<tr>
<td>National Industrial Security Program Operating Manual (NISPOM)</td>
<td>Prescribes requirements, restrictions, and safeguards to prevent unauthorized disclosure of classified information in industry</td>
</tr>
<tr>
<td>NISPOM Chapter 2</td>
<td>Provides information about facility clearances and personnel security clearances</td>
</tr>
<tr>
<td>DSS Facility Clearance Branch</td>
<td>Processes contractors for and issues facility security clearances; monitors contractor’s continued eligibility in the NISP</td>
</tr>
<tr>
<td>DSS Foreign Ownership, Control or Influence (FOCI) Operations Division</td>
<td>Resolves issues that arise when a cleared facility or a facility being processed for a facility clearance is subject to FOCI</td>
</tr>
<tr>
<td>Center for Development of Security Excellence (CDSE)</td>
<td>Provides security education and training to DoD and other U.S. government personnel and contractors</td>
</tr>
<tr>
<td>Facility Clearances in the NISP Course</td>
<td>Presents the requirements and process followed for a Facility Clearance to be granted and maintained</td>
</tr>
<tr>
<td>ISFD Facility Clearance Verification and Notifications for Industry Course</td>
<td>Provides step-by-step instructions on processing facility clearance verifications and notifications in the Industrial Security Facilities Database</td>
</tr>
<tr>
<td>Electronic Facility Clearance System (e-FCL)</td>
<td>System that all companies must use while in process for a facility clearance or to report a changed condition</td>
</tr>
</tbody>
</table>
Review Activity 1: Facility Clearance Resources

Which of these resources should you use to keep track of the tasks you need to perform to obtain a facility clearance?

Select the best response. Check your answer in the Review Activity Answer Key at the end of this Student Guide.

- Industrial Security Facility Database
- Facility Clearance Tracking Tool
- Facility Clearance Checklist
- A Guide for the Preparation of a DD Form 254

Learning Activity Introduction

In the Learning Activities that follow, you will practice using the resources available to you as an FSO. To answer the questions, find the appropriate resource on the Course Resources Page: http://www.cdse.edu/catalog/elearning/IS021-resources.html.

Learning Activity 1: Facility Clearance Resources

Read the question below. Then open the Course Resources Page and find the Facility Clearance Checklist. Select your response; then check your answer in the Learning Activity Answer Key at the end of this Student Guide.

What is the number that DSS uses to track basic facility information called?

- Facility Information Code
- NISP Number
- CAGE Code
- FSO ID Number
**Personnel Clearance Resources**

Now let’s consider some of the resources that are available to help you obtain and maintain personnel clearances for your company’s employees. You are already familiar with some such as the IS Rep, the NISPOM, PSMO-I, CDSE, the Personnel Clearances in the NISP Course, the JPAS/JCAVS Training for Security Professionals Course, and JPAS.

You will need additional resources as you help your employees through the personnel clearance process, and brief them about their responsibilities after they are cleared. Review each task below to learn about the resources associated with it.

**Assist in Obtaining Personnel Clearances**

To request a personnel security clearance, an employee must first complete Standard Form (SF) 86, Questionnaire for National Security Positions. An electronic version of this form is available through a JPAS interface called Electronic Questionnaires for Investigations Processing (e-QIP). When an employee transmits an SF 86 to you through e-QIP, you must review it for completeness, retain a hard copy, and then submit it to the Personnel Security Management Office for Industry (PSMO-I) through JPAS.

An OPM Personnel Security Investigator will use the information on the SF 86 as part of the employee’s background investigation. Using the DoD Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, the DoD Consolidated Adjudication Facility (CAF) will then decide whether to grant or deny the employee’s clearance request. You should be familiar with these guidelines, but you should not prejudge an employee based on them. The decision to grant or deny a clearance rests with the government. When the decision is made, the DoD CAF enters the employee’s eligibility for access to classified information into JPAS, and you are required to destroy the copy of the employee’s SF 86 that you saved.

**Brief Cleared Personnel**

Before you allow an eligible employee to actually access classified information, you must provide the employee with an initial security briefing about his or her responsibilities for safeguarding that information, and the employee must sign SF 312, Classified Information Nondisclosure Agreement.

The Information Security Oversight Office (ISOO) has prepared the Classified Information Nondisclosure Agreement Briefing Booklet to assist you. This booklet includes a brief discussion of the background and purpose of the SF 312, the text of pertinent legislative and executive authorizations, a series of questions and answers on its implementation, and a copy of the SF 312.
When you actually grant an employee access to classified information, you or another designated JPAS user at your facility must record that fact in JPAS.

**Previous Resources: Personnel Clearance Resources**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Defense Consolidated Adjudication Facility</td>
<td>Processes requests for personnel security clearances</td>
</tr>
<tr>
<td>(DoD CAF)</td>
<td></td>
</tr>
<tr>
<td>Joint Personnel Adjudication System (JPAS)</td>
<td>The DoD system for eligibility and access for personnel security clearances</td>
</tr>
<tr>
<td>Industrial Security Representative (IS Rep)</td>
<td>Represents DSS for security matters covered by the NISP; provides oversight, advice, and assistance to FSO</td>
</tr>
<tr>
<td>National Industrial Security Program Operating Manual</td>
<td>Prescribes requirements, restrictions, and safeguards to prevent unauthorized disclosure of classified information in industry</td>
</tr>
<tr>
<td>(NISPOM)</td>
<td></td>
</tr>
<tr>
<td>NISPOM Chapter 2</td>
<td>Provides information about facility clearances and personnel security clearances</td>
</tr>
<tr>
<td>Center for Development of Security Excellence (CDSE)</td>
<td>Provides security education and training to DoD and other U.S. government personnel and contractors</td>
</tr>
<tr>
<td>Personnel Security in the NISP Course</td>
<td>Provides an overview of personnel security in the National Industrial Security Program</td>
</tr>
<tr>
<td>JPAS/JCAVS Training for Security Professionals Course</td>
<td>Overview, detailed explanation, and hands-on training on JPAS and its subsystems</td>
</tr>
</tbody>
</table>
Review Activity 2: Personnel Clearance Resources

How are these personnel clearance forms used?

Match the form on the left to the appropriate description on the right. Check your answer in the Review Activity Answer Key at the end of this Student Guide.

| SF 86 Questionnaire for National Security Positions | A. Completed as part of an employee’s application for eligibility for a personnel clearance |
| SF 312 Classified Information Nondisclosure Agreement | B. Completed during an initial security briefing after an employee has been granted eligibility for a personnel clearance |

Learning Activity 2: Personnel Clearance Resources

Read the question below. Then open the Course Resources Page to look at an SF 312 to find your answer. Select your response; then check your answer in the Learning Activity Answer Key at the end of this Student Guide.

When completing an SF 312, what information must the employee provide in addition to his or her name, Social Security number, and dates?

- Date of birth
- Signature
- Telephone number
- Personnel clearance level
Security Education Resources

Now let’s look at some resources to help you with security education, awareness, and training. You have already seen so many that you may be wondering where to start.

To help you get your security education, training, and awareness program started, the DSS offers the Security Awareness for Educators (SAFE) Course, and job aids. Another good resource is the Online Guide to Security Responsibilities, which is a good source of material when preparing awareness briefings or articles for newsletters. Review the resources below to learn more.

SAFE Course

In the SAFE Course, you will learn how to create an effective security awareness and education program with a limited budget. This course identifies solutions for overcoming some of the challenges surrounding this responsibility, including how to gain management support for your program, how to motivate employees, and how to prepare and present effective security presentations.

Online Guide to Security Responsibilities

The Online Guide to Security Responsibilities allows you to create a unique security reference for your own use and, if you install it on your network, for all of your employees. The Guide’s user-friendly automated briefing system allows you to prepare security and threat awareness briefings, track which employees have taken them, and quiz employees on required security briefing material.

Previous Resources: Security Education Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Collection Trends in the U.S. Defense Industry</td>
<td>Reports on the foreign intelligence threat to facilities participating in the NISP</td>
</tr>
<tr>
<td>Industrial Security Representative (IS Rep)</td>
<td>Represents DSS for security matters covered by the NISP; provides oversight, advice, and assistance to the FSO; provides threat awareness information.</td>
</tr>
<tr>
<td>National Industrial Security Program Operating Manual (NISPOM)</td>
<td>Prescribes requirements, restrictions, and safeguards to prevent unauthorized disclosure of classified information in industry</td>
</tr>
<tr>
<td>NISPOM CHAPTER 3</td>
<td>Provides the basic requirements for FSO and cleared employee training</td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DSS Counterintelligence (CI) Office</td>
<td>Provides CI support through reviews, assessments, analysis, and reports</td>
</tr>
<tr>
<td>Center for Development of Security Excellence (CDSE)</td>
<td>Provides security education and training to DoD and other U.S. government personnel and contractors</td>
</tr>
<tr>
<td>Integrating CI and Threat Awareness Into Your Security Program Course</td>
<td>Will provide general threat awareness information and guidance on how to obtain CI support</td>
</tr>
<tr>
<td>Developing a Security Education and Training Program</td>
<td>Presents NISPOM security education, training, and awareness requirements and how to meet those requirements</td>
</tr>
<tr>
<td>Information Security Oversight Office</td>
<td>Issues binding directives for and monitors the NISP</td>
</tr>
<tr>
<td>Office of the National Counterintelligence Executive</td>
<td>Protects the U.S. intelligence community; thwarts adversarial intelligence directed against U.S. interests; provides threat awareness material</td>
</tr>
<tr>
<td>Defense Threat Reduction Agency</td>
<td>Safeguards the U.S. from weapons of mass destruction</td>
</tr>
<tr>
<td>Interagency OPSEC Support Staff</td>
<td>Helps government organizations develop operations security programs and provides threat awareness information</td>
</tr>
<tr>
<td>Federal Bureau of Investigation</td>
<td>Helps protect U.S. communities and businesses from terrorism and domestic espionage and provides threat awareness information</td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Protects U.S. transportation systems and provides threat awareness information</td>
</tr>
<tr>
<td>Department of State</td>
<td>Promotes democracy in the international community and provides threat awareness information</td>
</tr>
<tr>
<td>Directorate of Defense Trade Controls</td>
<td>Controls export and temporary import of defense articles and services covered by the United States Munitions List</td>
</tr>
</tbody>
</table>
Review Activity 3: Security Education Resources

Which of the following can you do with the Online Guide to Security Responsibilities?

Select all that apply. Check your answer in the Review Activity Answer Key at the end of this Student Guide.

- Order threat awareness videos and posters
- Track which briefings each employee has seen
- Learn how to motivate employees
- Create a security reference guide that is unique to your organization
- Prepare security and threat awareness briefings
- Quiz employees on what they have learned in automated security briefings

Learning Activity 3: Security Education Resources

Read the question below. Then open the Course Resources Page to see the NISPOM, and consult it to find the answer. Select your response; then check your answer in the Learning Activity Answer Key at the end of this Student Guide.

Which of the following best describes the FSO training requirements in the NISPOM?

- CDSE is responsible for ensuring that FSOs are trained within six months of appointment.
- Contractors are responsible for ensuring that FSOs are trained within six months of appointment.
- Contractors are responsible for ensuring that FSOs are trained within one year of appointment.
- CDSE is responsible for ensuring that FSOs are trained within one year of appointment.
Safeguarding Resources

Now let’s look at some resources to help you protect classified information. You have learned about a number of resources to help you in this role. You may recall, however, that not all facilities need the same resources. The resources you need will depend on whether your facility generates classified information, whether your facility stores classified information, whether anyone in your facility is required to transmit or transport classified materials, and whether your facility has a classified information system. Review each category below to learn more about the resources available for different types of facilities.

Resources for Facilities that Generate Classified Materials

If your facility generates classified information, you need to understand how information is classified and how classified materials are marked. You have already been introduced to some of the resources available to help you such as your IS Rep, the NISPOM, DD Form 254, the Atomic Energy Act, E.O. 13526, the GCA, the Center for Development of Security Excellence, the Derivative Classifications Course and the Marking Classified Information Course.

A uniform security classification system for classifying and marking documents is prescribed in Executive Order 13526 and the Atomic Energy Act of 1954, as amended. The identification and markings provisions of the implementation guidance to the Executive Order became effective when ISOO issued 32 CFR, Parts 2001 and 2003 Final Rule. In addition, ISOO also issued its marking booklet which provides comprehensive guidance on identifying and marking classified documents.

Resources for Facilities that Store Classified Materials

You have already learned about resources to help you protect classified information such as your IS Rep, the NISPOM, DD Form 254, the GCA, the Center for Development of Security Excellence, and the Safeguarding Classified Information in the NISP Course.

If your company stores classified materials, then you should also know about the DoD Lock Program, which provides information about and technical support for required locks, safes, vaults, seals, and containers. When you store classified documents, you must also meet government shredding requirements to dispose of them.

Check the Evaluated Products List for information about these requirements and for specific products that meet them.
Resources for Facilities that Transmit & Transport Classified Materials

If personnel at your facility must transmit or transport classified materials outside the facility, they must follow special procedures. The domestic delivery services approved for overnight domestic delivery of Secret and Confidential information are listed in a job aid called Transportation, Delivery, and Relocation Solutions (TDRS). It is recommended that you complete the Transmission and Transportation for Industry Course from CDSE to learn more about this topic.

Resources for Facilities with Classified Information Systems

If your facility has classified information systems, you and others at your facility will need additional training as follows:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NISPOM Chapter 8 Implementation Course</td>
<td>Covers the DSS/ODAA Certification and Accreditation (C&amp;A) Process, including configuration of computers based on the security standards in Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM) and the Standardization of Baseline Technical Security Configurations (published by DSS)</td>
</tr>
<tr>
<td>Information System Security in the National Industrial Security Program (ISS-NISP) (Instructor-led)</td>
<td></td>
</tr>
<tr>
<td>Introduction to the NISP C&amp;A Process Course</td>
<td>Introduces the NISP certification and accreditation process to include training on the policies and standards used to protect information within computer systems, identifying and defining the Government and contractor roles and the risk management process as it relates to the C&amp;A process</td>
</tr>
<tr>
<td>NISP C&amp;A Process: A Walk-Through Course</td>
<td>This course is a continuation of the Introduction to the NISP C&amp;A Process Course and it identifies in depth the individual phases of the DSS C&amp;A process</td>
</tr>
<tr>
<td>Technical Implementation of Certification and Accreditation (C&amp;A) - Configuration to DSS Standards Course</td>
<td>This course focuses on more technical aspects of the C&amp;A process and guides students on navigating through the system using the Baseline Technical Security Configuration Guide</td>
</tr>
</tbody>
</table>
### Resource Description

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Implementation of Certification and Accreditation (C&amp;A) - Configuration to DSS Standards Virtual Environment</td>
<td>This course provides guidance on the technical aspects of the C&amp;A process and provides students an opportunity to practice what they have learned in a non-production/test environment</td>
</tr>
</tbody>
</table>

### Review Activity 4: Safeguarding Resources

Which of these resources do you need to help you generate classified documents?

Select the best response. Check your answer in the Review Activity Answer Key at the end of this Student Guide.

- Marking Classified National Security Information
- Generating Classified National Security Information
- Transportation, Delivery, and Relocation Solutions
- Evaluated Products List

### Learning Activity 4: Safeguarding Resources

Read the question below. Then open the Course Resources Page to view the Marking Classified National Security Information booklet and read about the “primary markings” required on classified documents. Write your response in the space below; then check your answer in the Learning Activity Answer Key at the end of this Student Guide.

What are the essential markings for a classified document?
Self-Inspection Resources

Now let's look at the resources you are likely to use as you inspect your facility to ensure that your facility is meeting the NISP requirements and protecting classified information. CDSE provides two useful job aids to help you as you conduct the self-inspections that are required under the NISP which are:

- Self Inspection Handbook for NISP Contractors
- Suggested Contract File Folder Headings

Review information about each job aid below to learn more.

Self Inspection Handbook for NISP Contractors

The Self Inspection Handbook for NISP Contractors is designed to help you conduct self-inspections to ensure that your facility is meeting the NISP requirements and protecting classified information in compliance with the NISPOM.

This handbook includes numerous checklists, as well as techniques to help you enhance the quality of your self-inspections.

Suggested Contract File Folder Headings

This job aid includes a list of files and records that you should consider when establishing your file and record keeping system. Some of these records are required and some are recommended.

Previous Resources: Self-Inspection Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Security Representative (IS Rep)</td>
<td>Represents DSS for security matters covered by the NISP; provides oversight, advice, and assistance to the FSO</td>
</tr>
<tr>
<td>National Industrial Security Program Operating Manual (NISPOM)</td>
<td>Prescribes requirements, restrictions, and safeguards to prevent unauthorized disclosure of classified information in industry</td>
</tr>
<tr>
<td>Center for Development of Security Excellence (CDSE)</td>
<td>Provides security education and training to DoD and other U.S. government personnel and contractors</td>
</tr>
<tr>
<td>NISP Self Inspection Course</td>
<td>Introduces the requirements to conduct self inspections</td>
</tr>
</tbody>
</table>
Review Activity 5: Self-Inspection Resources

Which of the following best describes the Self Inspection Handbook for NISP Contractors?

Select the best response. Check your answer in the Review Activity Answer Key at the end of this Student Guide.

- A policy document that states the requirements for periodic self-inspections
- A schedule for self-inspections and vulnerability assessments
- A list of files and records that you should maintain
- A job aid designed to help you prepare for self-inspections

Learning Activity 5: Self-Inspection Resources

Read the question below. Then open the Course Resources Page and view the Self Inspection Handbook for NISP Contractors to find the answer. Select your response; then check your answer in the Learning Activity Answer Key at the end of this Student Guide.

What is the MINIMUM number of “elements of inspection” that you must cover in a facility self-inspection?

- 1
- 3
- 6
- 10
**Reporting Resources**

You have already learned about the types of events and information you are required to report to the government. So you should be familiar with the following organizations and resources: your IS Rep, the NISPOM, the FBI, PSMO-I, the Center for Development of Security Excellence, the NISP Reporting Requirements Course, JPAS, and the Adjudicative Guidelines.

In addition, you and your employees should know that each Cognizant Security Agency (CSA) has a hotline. Any government or contractor employee can use these hotlines to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects.

**Learning Activity 6: Reporting Resources**

Read the question below. Then open the [Course Resources Page](#) to find the hotline numbers under the category Contact Info. Select your response; then check your answer in the [Learning Activity Answer Key](#) at the end of this Student Guide.

What is the CSA hotline number for the Department of Defense?

- (800) 424-9098
- (202) 286-4073
- (800) 586-4073
- (800) 233-3497

**Lesson Conclusion**

In this lesson, you were introduced to many different types of the resources available to help you fulfill your responsibilities as an FSO, and you learned about how you can access those resources.
Answer Key

**Review Activity 1: Facility Clearance Resources**

To keep track of the tasks you need to perform in order to obtain a facility clearance, you need the **Facility Clearance Checklist**.

Here is an explanation of why the other responses are incorrect:

- The ISFD tracks the status of a request for facility clearances.
- There is no such resource as a Facility Clearance Tracking Tool.
- The Guide for Preparation of a DD Form 254 can help you provide contract-specific guidance to your subcontractors after you have obtained a facility clearance.

**Review Activity 2: Personnel Clearance Resources**

SF 86, Questionnaire for National Security Positions, is completed as part of an employee's application for eligibility for a personnel clearance. After employees have been granted eligibility, and before they have been granted access to classified information, they must receive an initial briefing and execute SF 312, Classified Information Nondisclosure Agreement.

**Review Activity 3: Security Education Resources**

You can use the Online Guide to Security Responsibilities to create a unique reference, to create briefings, and to track employees’ understanding of those briefings. You can learn how to motivate employees by taking the SAFE Course.

**Review Activity 4: Safeguarding Resources**

To generate classified documents, you need to know how to mark them properly. The **Marking Classified National Security Information booklet** is a good source of guidance for this task.

**Review Activity 5: Self-Inspection Resources**

The Self Inspection Handbook for NISP Contractors is a job aid designed to help you prepare for self-inspections. This handbook includes self-inspection checklists and techniques to improve the quality of your self-inspections.
Learning Activity 1: Facility Clearance Resources

On the Facility Clearance Checklist, you can see that the DSS uses a Commercial and Government Entity (CAGE) Code to track basic facility information. If your facility does not have a CAGE Code, you need to go online to obtain one.

Learning Activity 2: Personnel Clearance Resources

Employees must provide their names, signatures, dates, and Social Security numbers on SF 312.

Learning Activity 3: Security Education Resources

In the Table of Contents of the NISPOM, you'll see that FSO Training is covered in paragraph 3-102. There you will find that contractors are responsible for ensuring that FSOs are trained within one year of their appointment.

Learning Activity 4: Safeguarding Resources

Sections 1 and 2 of the Marking Classified National Security Information booklet tells you that the primary markings for a classified document are:

- Portion markings
- Overall Classification Markings
- Classification authority block
- Declassification instructions

Learning Activity 5: Self-Inspection Resources

In this Handbook, you would read that at least three elements of inspection must be covered in a self-inspection by all facilities: Facility Security Clearance, Access Authorizations, and Security Education.

Learning Activity 6: Reporting Resources

The hotlines are used to report violations of ethical standards and/or the law, including but not limited to fraud, waste, or abuse of authority, potential leaks of classified information, or potential acts of terrorism.
Lesson Introduction

You have learned a lot about the roles and responsibilities of the Facility Security Officer (FSO) in the National Industrial Security Program (NISP). Most importantly, you have learned that the NISP is a partnership between the government and industry. The government supplies numerous resources to support your implementation of NISP requirements, and your Industrial Security Representative (IS Rep) is always available for guidance.

This lesson will allow you to practice some of the skills you will need as an FSO, using scenarios that you may encounter in real life. As this lesson opens, PRIME, Incorporated is about to join the NISP and you have been designated as the company’s FSO. As a new FSO, you are not expected to know the answers to all the questions that are posed to you, but you are expected to use the resources available to find as many answers as you can. As you work your way through the scenarios, it would be optimal for you to access the Course Resources Page (http://www.cdse.edu/catalog/elearning/IS021-resources.html) or CDSE website (www.cdse.edu) at any time, and your IS Rep will be available with hints.

*IS Rep Hint: Your IS Rep is here to help you, so if you’re stuck, don’t be afraid to see what your IS Rep has to say.*

When you are finished with each activity, see the Learning Activity Answer Key at the end of this Student Guide to check your answers.
**Learning Activity 1: Getting Ready for the IS Rep**

Read the scenario and question. Use the Course Resources Page to find the information you need.

**Scenario:** Defense Security Service (DSS) has begun the facility clearance process for PRIME, Inc., and you have received a package of important information. Your IS Rep called and introduced herself. She will be making her first visit to your facility soon, and wants you to prepare the proper documentation before she comes.

Which of the following are you NOT required to provide?

*Select the best answer to the question.*

- Key Management Personnel list
- Prime Inc.’s Federal Tax ID Number
- Resumes for personnel who will need security clearances
- Proof of citizenship for yourself (the FSO)

**IS Rep Hint:** Find the Facility Clearance Checklist on the Course Resources Page.

**Learning Activity 2: Check on Facility Clearance**

Read the scenario and question. Use the Course Resources Page to find the information you need.

**Scenario:** Your IS Rep is working with the DSS Facility Clearance Branch to help you obtain your facility clearance. You have received an interim FCL, and the President of PRIME, Inc. wants to know the final status of your clearance, so you access the Industrial Security Facilities Database (ISFD).

What resources are available to help you with the ISFD?

*Write your answer(s) in the space provided.*

**IS Rep Hint:** Don’t forget to check the CDSE website.
Contract Award

Congratulations! PRIME, Inc. has received a Secret facility clearance and has been awarded a contract. The DD Form 254, Department of Defense Contract Security Classification Specification, provides contract-specific guidance that you may need later.

Learning Activity 3: Deciding Eligibility

Which organization grants eligibility to a contractor employee to have access to classified information?

Select the best response.

- Foreign Ownership, Control or Influence Division
- Department of Defense Consolidated Adjudications Facility
- Office of the Designated Approving Authority
- Office of Personnel Management

*IS Rep Hint: Two of these organizations will be involved in the personnel clearance process, but it will be a DSS organization that makes the decision.*

Learning Activity 4: Grant Access

Read the scenario and question. Use the NISPOM on the Course Resources Page to find the information you need.

Scenario: The DoD CAF has granted all three of your new employees eligibility for access to classified information and entered that eligibility into JPAS. The President of PRIME is anxious for them to start work.

What other tasks must be completed before the newly eligible employees may begin working with classified information?

Select the best answer(s).

- Conduct initial security briefing
- Sign SF 312, Nondisclosure Agreement
- Complete a Financial Disclosure Form
- Conduct a polygraph examination

*IS Rep Hint: If you don’t remember the answer to this question, it might be tricky. Look at paragraphs 3-105 and 3-106 in the NISPOM.*
Learning Activity 5: Conduct Initial Briefing

Read the scenario and question. Use the Course Resources Page to find the information you need.

Scenario: After the DoD CAF granted your employees’ eligibility for access to classified information, you used a job aid associated with SF 312 to conduct an initial briefing for each of them. At the end of the briefing, they each executed SF 312. According to the job aid, however, there is one more requirement before an employee may have access to classified information.

According to the job aid associated with SF 312, what is the third requirement that an employee must meet before he or she can access classified information?

Select the best answer to the question.

- Pass a polygraph test
- Pass a physical examination
- Present two character references
- Have a need to know

IS Rep Hint: Use the Course Resources Page to find the Classified Information Nondisclosure Agreement Briefing Booklet (SF 312).

Learning Activity 6: What if….Refusal to Sign

Read the scenario and question. Use the NISPOM on the Course Resources Page to find the information you need.

Scenario: One of your eligible employees will not sign the SF 312.

What course of action should you take?

Select the best answer to the question.

- Fire the employee
- Send the employee for counseling
- Report the employee to the FBI
- Report the employee to PSMO-I

IS Rep Hint: See NISPOM paragraph 1-302 f.
**Learning Activity 7: Generate Classified Documents**

Read the scenario and question. Use the CDSE Course Catalog on the [CDSE website](http://www.cdswebsite.com) to find the information you need.

**Scenario:** Your employees will be generating classified documents as part of the contract.

What courses should your employees take to learn about generating classified documents?

*Select the best answer.*

- Categorizing Classified Information Course
- Derivative Classification Course
- Original Classification Course
- Personally Identifiable Information (PII) Course

**IS Rep Hint:** Use the CDSE Course Catalog on the [CDSE website](http://www.cdswebsite.com) to find out what courses are available.

**Learning Activity 8: Understand Derivative Classification**

Read the scenario and question. Use the NISPOM on the [Course Resources Page](http://www.coursesresourcespage.com) to find the information you need.

**Scenario:** Your IS Rep tells you that marking classified information requires a good understanding of derivative classification.

Which of the following is the best definition of derivative classification?

*Select the best answer.*

- The act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information
- The act of deriving the appropriate overall classification level of a document by looking for the highest level classification of any of the portion markings
- The act of individually classifying paragraphs, charts, tables, pictures, illustrations, subjects, and titles
**FSO Role in the NISP**

**Final Learning Activity**

*IS Rep Hint: To find this definition you can look in Appendix C of the NISPOM.*

**Learning Activity 9: Investigate Locks**

Read the scenario and question. Use the [Course Resources Page](#) to find the information you need.

**Scenario:** Your GSA container is equipped with the X-09 lock. It was working fine yesterday but today the dial is hard to turn. Where can you find help?

How can the DoD Lock Program assist you?

Write your answer(s) in the space provided.

*IS Rep Hint: Search the frequently asked questions section on the DoD Lock Program website.*
**Learning Activity 10: Verify Clearances**

Read the scenario and question. Use the NISPOM on the [Course Resources Page](#) to find the information you need.

**Scenario:** Your employees need to host visitors at your facility to discuss the classified contract. The NISPOM includes policy about classified visits.

What must you verify before you receive visitors for classified visits?

*Select the best answer to the question.*

- The visitors’ citizenship
- The visitors’ names, dates of birth, and Social Security numbers
- The visitors’ fingerprint identifications
- The visitors’ personnel clearances and need-to-know

**IS Rep Hint:** Look in NISPOM Chapter 6 VISITS AND MEETINGS.

**Learning Activity 11: What if.....Hurricane**

Read the scenario and question. Use the NISPOM on the [Course Resources Page](#) to find the information you need.

**Scenario:** A hurricane knocked out your power. It’s expected to be out for three days and you don’t think you will be able to secure the building.

What should you do?

*Select the best answer to the question.*

- Report the situation to your IS Rep
- Report the situation to the FBI
- Report the situation to PSMO-I

**IS Rep Hint:** See NISPOM paragraph 1-302 i.
Learning Activity 12: What if…..Stock Purchase

Read the scenario and question. Use the NISPOM on the Course Resources Page to find the information you need.

Scenario: A Japanese company is buying 51 percent of the stock of PRIME, Inc.

What should you do?

Select the best answer to the question.

- Report the situation to the DSS FOCI Division
- Report the situation to your IS Rep
- Report the situation to the FBI
- Report the situation to PSMO-I

IS Rep Hint: See NISPOM paragraph 1-302 g and section 2-3.

Learning Activity 13: Prepare for Review

Read the statement. Look in the NISPOM on the Course Resources Page to see if it is true of false.

Statement: The NISPOM requires that you conduct periodic self-inspections to insure your facility is meeting the requirements of the NISP and adequately protecting classified information.

Is the above statement True or False?

Select True or False.

- True
- False

IS Rep Hint: Look at NISPOM paragraph 1-206 b.
Learning Activity 14: Conduct Self-Inspection

Read the scenario and question. Use the Course Resources Page to find the information you need.

Scenario: You schedule a self-inspection midway between your scheduled government security vulnerability assessment. What are some techniques that you should use when you interview your employees during a security self-inspection?

Write your answer(s) in the space provided.

IS Rep Hint: Find the Self Inspection Handbook for NISP Contractors. It is a job aid used by FSOs in the industrial security discipline.

Congratulations!
Your self-inspection turned up a few areas for improvement. You and your staff worked together with your IS Rep to correct those areas, and the result of the security vulnerability assessment for Prime, Incorporated was a “Satisfactory” rating by your IS Rep.

Lesson Conclusion
This lesson has allowed you to practice the skills you will need as an FSO. Your job is complex and you are not expected to know all the answers, but if you are familiar with the resources available, and know where to go when you need help, you will succeed in all of your roles.
Answer Key

**Learning Activity 1: Get Ready for IS Rep**

Find the Facility Clearance Checklist on the Course Resources Page. This Checklist includes the documentation you must prepare:

- Articles of Incorporation, stock records, minutes of board meetings, corporate by-laws
- Federal Tax ID Number
- 10K Reports
- Key Management Personnel list
- Summary of your company’s primary business
- Email, fax, and address information for the last 10 years
- Proof of US citizenship for the FSO

Did you notice that the Checklist also tells you to download the NISPOM?

**Learning Activity 2: Check on Facility Clearance**

The Course Resources Page provides access to the ISFD login screen. You can access the Industrial Security Facilities Database (ISFD) Facility Clearance Verification and Notifications for Industry v3 course from the CDSE website.

**Learning Activity 3: Deciding Eligibility**

*Department of Defense Consolidated Adjudications Facility (DoD CAF)* uses Adjudicative Guidelines and information from the Office of Personnel Management (OPM) background investigation to decide who is eligible for access to classified information.
**Learning Activity 4: Grant Access**

This is a policy question, and the answer is in the NISPOM, but it is not in the section on personnel clearances. Paragraph 3-105 (in the chapter on security training and briefings) states: “An employee issued an initial PCL must **execute an SF 312** prior to being granted access to classified information.”

Paragraph 3-106 provides guidance on the **initial security briefing that must be completed** prior to the employee having access to classified information.

SF 312 is the Classified Information Nondisclosure Agreement that employees execute as part of their initial security briefing.

**Learning Activity 5: Conduct Initial Briefing**

In the Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet, under Background and Purpose, you will find the three requirements for access to classified information: a clearance, an executed SF 312, and a **“need to know”**. The onus for determining need to know is on the holder of the classified information.

**Learning Activity 6: What if…Refusal to Sign**

NISPOM paragraph 1-302 f requires you to report an employee’s refusal to sign the SF 312 to your Cognizant Security Agency (CSA). When your CSA is the Department of Defense and the reportable matter is personnel-related, you usually **report it to the Personnel Security Management Office for Industry (PSMO-I)**. Do not grant the employee access to classified information.

**Learning Activity 7: Generate Classified Documents**

You can use the course catalog to find out what courses are available. You would find that CDSE offers a **Derivative Classification Course** that covers how to generate classified documents.

**Learning Activity 8: Understand Derivative Classification**

To find definitions in the National Industrial Security Program, you can **look in Appendix C of the NISPOM**, which is a glossary of terms related to industrial security.
**Learning Activity 9: Investigate Locks**

In addition to the DoD Lock Program Technical Support Hotline staff that can help you with information on security hardware selection, requirements, specifications, national stock numbers, purchasing, training, and troubleshooting of equipment failures; there is also a list of **Frequently Asked Questions** that may be of assistance.

**Learning Activity 10: Verify Clearances**

NISPOM paragraph 6-104 specifies the requirements for obtaining visit authorizations for a classified visit. You must verify **the visitors’ personnel clearances** by reviewing a “CSA-designated database” or by requesting a visit authorization letter that contains the necessary information. For DoD contractors, the CSA-designated database for this purpose is JPAS.

NISPOM paragraph 6-102 states that the responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit.

**Learning Activity 11: What if……Hurricane**

You should report an inability to safeguard classified material to your IS Rep and make arrangements to provide appropriate protection of the material until normal operations are restored. This type of emergency situation is covered in NISPOM paragraph 1-302 i.

**Learning Activity 12: What if…..Stock Purchase**

You should report changes in ownership, including stock transfers that affect control of the company, to your IS Rep. This is covered in NISPOM paragraph 1-302 g. This would be required even if the buyer were American. Since the buyer is foreign, your IS Rep will probably consult with the DSS FOCI Division to resolve any issues of foreign ownership, control or influence, and will ask you for additional information.

**Learning Activity 13: Prepare for Review**

This statement is true. Self-inspections are required, by **NISPOM paragraph 1-206 b.**
Learning Activity 14: Conduct Self-Inspection

You could have found the Self Inspection Handbook for NISP. The handbook is accessible as a PDF file, so you can browse through it or search for specific information in it, including these interview techniques:

- All questions should be considered in the present and future tense.
- Let people tell their story. Ask open-ended questions (using who, what, where, when, why, and how).
- Let people show you how they perform their job while handling classified information.
- Follow-up the check list questions with your own questions.
- Keep good notes for future reference and corrective action.
Lesson 6: Course Conclusion

Course Summary

The National Industrial Security Program (NISP) plays a significant role in protecting our national security, and the Facility Security Officer (FSO) is a central player in this program. You should now be familiar with the roles and responsibilities of the FSO in the NISP and with many of the resources available to help you fulfill those responsibilities.

Lesson Review

Here is a list of the lessons in the course.

- Roles and Responsibilities
- Policy Guidance and Reporting Requirements
- Resources
- Final Learning Activity

Course Objectives

You should now be able to:

- Identify the purpose of the National Industrial Security Program (NISP)
- Identify roles and responsibilities in the NISP
- Identify the structure and requirements of the National Industrial Security Operating Manual (NISPOM)
- Identify and access resources available to the Facility Security Officer (FSO)
- Identify government personnel who will work with the FSO to meet the requirements of the NISP

Conclusion

Congratulations on completing the Facility Security Officer Role in the National Industrial Security Program Course.
To receive course credit, you MUST take the FSO Role in the NISP examination. Please use the STEPP system to register for the online exam.

Although not required by the NISPOM, you are now eligible to enroll in the instructor-led, FSO Getting Started Seminar for New FSOs.