Introduction to Industrial Security, v3

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Introduction

Subcontractor CEO: I'm really excited -- my company, BuildGen Contracting, just won our first classified subcontract! But now we need to make sure we establish an effective security program to protect classified information. Where do we begin?

Prime Contractor FSO: Congratulations! We look forward to working with you on this effort! There are several steps you and your company will need to take before you can access classified information under this contract, and there's a lot of information that you will need to be aware of.

Main Narrator: Whether you work for a company that is working on its first classified contract or a company with existing classified contracts, protecting classified information is a priority for all government and industry employees. Did you know that much of all U.S. classified information is developed by industry? Every day, contractors have access to classified and Controlled Unclassified Information, or CUI, as well as government facilities, information systems, and equipment.

With that in mind, you can see the need to have security guidelines and procedures that are closely monitored, with one goal in mind—to protect our national security by providing for the security of our sensitive and classified information.

Welcome to the Introduction to Industrial Security course.

Objectives

This course will provide an overview of the National Industrial Security Program, or NISP, including its purpose and structure, key roles, the classified contracting process and contract requirements, and the basic security clearance processes and requirements.

These topics are very broad, so when there is an opportunity for you to learn more, the course will direct you to additional courses that will be helpful.

Here are the course objectives. Take a moment to review them.

- Recognize the role of the National Industrial Security Program (NISP) in the protection of classified information entrusted to industry
- Describe government and contractor security roles and responsibilities in accordance with the NISP Operating Manual (NISPOM)
- Outline the process and requirements for establishing a classified contract

- Identify the security clearance processes and procedures required for access to classified information

Lesson 2: Overview of the NISP

Introduction

Objectives

Subcontractor CEO: I need more help with the NISP. I'm not sure I understand how it applies to my new classified contract and all that may be involved or expected of us.

Prime Contractor FSO: The NISP, or National Industrial Security Program, is the program that oversees the safeguarding of classified information used by cleared contractors, like our companies. It defines the requirements, restrictions, and other safeguards that prevent the unauthorized disclosure of classified information, and it oversees their implementation.

Main Narrator: This lesson will provide an overview of the purpose and structure of the NISP, and its role in safeguarding classified information entrusted to industry.

Here are the lesson objectives. Take a moment to review them.

- Identify the purpose of the National Industrial Security Program (NISP)
- Recognize the role of the NISP Operating Manual (NISPOM)
- Define Cognizant Security Agencies (CSAs) and Cognizant Security Offices (CSOs)
- Identify the role of CSAs and CSOs in the NISP
- Identify the role the Defense Security Service (DSS) plays in NISP administration and oversight

What is the NISP?

Purpose of the NISP

The majority of our nation's technology is developed and produced by industry – and much of that technology is classified. The U.S. Government entrusts cleared contractor facilities with access to classified and Controlled Unclassified Information, or CUI, government facilities, information systems, and equipment.

The National Industrial Security Program, or NISP, is a Government-Industry partnership established in 1993 by Executive Order 12829. The NISP ensures that cleared industry safeguards classified information in its possession. Within the NISP, the government establishes the requirements for the protection of classified information, and industry implements these requirements with the government's advice, assistance, and oversight.

The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities in the United States, and is designed to be cost effective and efficient.

It defines the requirements, restrictions, and other safeguards designed to prevent unauthorized disclosure of classified information and calls for close monitoring of these critical guidelines and procedures.

NISP Operating Manual

The Department of Defense, or DoD, Regulation 5220.22-M, more commonly referred to as the National Industrial Security Program Operating Manual, or NISPOM, defines the requirements, restrictions, and safeguards that industry must follow.

The NISPOM provides guidance so that security can be implemented uniformly across a wide range of contractors, but it is also general enough that it may be customized for each contractor's situation and needs.

NISPOM topics include:

- General policies and procedures
- Reporting requirements
- Facility Clearances (FCLs)
- Personnel Security Clearances (PCLs)
- Foreign Ownership, Control, or Influence (FOCI) issues
- Security training and briefings
- Classification
- Marking requirements
- Safeguarding of classified information
- Visits and meetings
- Subcontracting
- Information System (IS) security
- Special requirements, including nuclear-related information, Critical Nuclear Weapon Design Information (CNWDI), intelligence information, and Communications Security (COMSEC)
- International security requirements

Classified and Sensitive Unclassified Contracts

When industry provides a service to the government, all security details must be covered in the contract, including requirements for safeguarding classified information and what level of clearance employees involved in the contract will need, among other concerns. This security guidance must be adhered to by the contractor and all of its employees.

Although the NISP only covers contracts that involve classified materials, unclassified contracts can still involve critical or sensitive information that requires safeguarding, such as Personally Identifiable Information, or PII, or budgets.

For both classified information and CUI, contracts must identify the security requirements and how the contractor will be reimbursed for associated costs. Contracts can specify additional security requirements that go above and beyond what the NISPOM requires but classified contracts can never be less restrictive than what is required by the NISPOM.

Structure of the NISP

Government and Industry Responsibilities

In order to implement the NISP and protect classified information, government agencies and industry contractors play important but distinct roles.

On the government side, Cognizant Security Agencies, or CSAs, establish general industrial security programs and oversee and administer security requirements. Each CSA has one or more Cognizant Security Offices, or CSOs, which administer the NISP on their behalf.

For a specific contract, the Government Contracting Activity, or GCA, represents the agency that issues the contract. The GCA provides industry with contract-specific security classification guidance. The GCA has broad authority regarding acquisition functions for its agency, as delegated by the agency head. The designation of a CSO does not relieve the GCA of its responsibility to protect and safeguard classified information. Security requirements outside the scope of the NISP require oversight from the government agency or organization that levied those requirements upon the contract.

Finally, based on their classified involvement in the NISP, industry has one major responsibility: they must implement the applicable NISPOM requirements needed to protect classified information.

CSAs and CSOs

CSAs, are those agencies authorized by Executive Order 12829 to establish industrial security programs and oversee and administer security requirements.

There are five CSAs that are ultimately responsible for the security of all cleared U.S. contractors. The Department of Defense, or DoD, is the largest CSA with the most classified contracts with industry. Other CSAs include the Office of the Director of National Intelligence, or ODNI, the Department of Energy, or DoE, the Nuclear Regulatory Commission, or NRC, and the Department of Homeland Security, or DHS. Each CSA has one or more Cognizant Security Offices, or CSOs, which administer the NISP.

The Defense Security Service, or DSS, has been designated as the CSO for the DoD and over 30 other non-DoD agencies, including DHS, who have entered into agreements with the DoD. You can view a list of agencies with DSS agreements on the DSS website. Depending on the security requirements of the classified programs involved, other government agencies may also assume some of the CSO functions.

DoD Delegation of Security Cognizance

As you just learned, the DoD is the largest of the CSAs, and it delegates security cognizance to DSS as its CSO.

As CSO, DSS administers the NISP; provides security guidance, oversight, and policy clarifications; and conducts periodic Security Vulnerability Assessments, or SVAs, to ensure adherence to the NISPOM and contract guidelines.

DSS is responsible for the oversight of all NISPOM requirements. Some of the more common security elements that DSS oversees as CSO include: storage of classified information; visit procedures; security awareness and training; procedures for protecting classified on Information Systems, or ISs; Personnel Security Clearances, or PCLs, for employees working on classified contracts; any changes in ownership, management, or foreign involvement; and compliance with reporting requirements.

Security Cognizance Considerations

DSS oversees U.S. cleared contractor facilities participating in the NISP. Some of these companies access classified information at their own facilities and some access classified information at another cleared contractor or government or agency site. Regardless of where their access takes place, all cleared contractors must follow the applicable security procedures, as documented in the NISPOM.

DSS might not have security oversight for classified contract work being performed on a government installation. Those contracts may have different requirements from classified contract work performed at the contractor's own cleared facility or at another cleared contractor site, and contractors working on government installations or agency sites must follow all standard operating procedures for the installation or agency. These procedures may be more restrictive but should never be less restrictive than what the NISPOM requires, must be clearly outlined in the contract, and are typically established and overseen by the installation commander, who has security cognizance in accordance with DoD 5220.22-R, the Industrial Security Regulation. The installation commander or head of the User Agency, or UA, can request in writing that DSS assume cognizance.

Note that if the contractor is performing entirely unclassified work on a military installation, DSS is not involved, although in some cases, additional security requirements may appear in the contract.

Finally, note that when cleared contractors work on a Special Access Program, or SAP, the Program Manager may retain some of the CSO's responsibilities.

Information Systems Security

Classified Information Systems, or ISs, can be important assets with significant implications for national security. Many store large amounts of valuable information and need continuous

protection. Contractors may operate their own ISs, they may use government-owned systems at the government or agency site, or they may use a government-owned system at their own cleared contractor site.

Contractors operating their own systems must follow the provisions laid out in chapter 8 of the NISPOM. Contractors accessing government-owned systems at the government site must follow the security provisions outlined by the owner of the system, and these provisions and requirements must be specified in the contract. And in cases where contractors operate government-owned systems at the contractor site, the requirements of NISPOM Chapter 8 take precedence.

Lesson 2 Review Activities

Review Activity 1

Contractor CEO: My company, BuildGen Contracting, just won its first classified government contract. What are our NISP responsibilities?

What are contractor responsibilities according to the NISP?

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

- ○ Establish NISP requirements for the protection of classified information
- ○ Provide advice, assistance, and oversight
- ○ Implement NISP requirements for the protection of classified information

Review Activity 2

Contractor CEO: Can you help me understand what the difference is between CSAs and CSOs?

Identify whether the following statements describe CSAs or CSOs. Check your answer in the Answer Key at the end of this Student Guide.

These organizations establish industrial security programs and oversee security requirements.

- ○ CSA
- ○ CSO

These organizations administer the NISP and provide security guidance, oversight, and policy clarifications.

- ○ CSA
- ○ CSO

Review Activity 3

Contractor CEO: I understand DSS will be the CSO for our company. What will they do for us?

Which of these are DSS responsibilities or functions?

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

- ☐ Provide security guidance and oversight
- ☐ Provide policy clarifications
- ☐ Conduct Security Vulnerability Assessments (SVAs)
- ☐ Provide installation-specific procedures for work performed on a government installation
- ☐ Provide contract-specific security classification guidance

Lesson 3: Security Roles in the NISP

Introduction

Objectives

Subcontractor CEO: Okay, so now I understand the basic structure of the NISP… but I still have some questions. Is there someone I can talk to?

Prime Contractor FSO: Yes, there are several individuals in government roles who are assigned to help contractors like you navigate the NISP and ensure classified information is protected.

Main Narrator: Recall that in order to protect classified information, government agencies and industry both have a role to play in the NISP. Within each of these organizations, different individuals do their part to make sure that classified information is protected.

Here are the lesson objectives. Take a moment to review them.

- Recognize the main government security roles described in the NISPOM
- Recognize the main contractor security roles described in the NISPOM
- Identify how government and contractor personnel work together to ensure the security of information used in classified contracts

Organizational Roles and Responsibilities

DSS Mission: Regional NISP Administration

Before exploring the roles that individuals play in the NISP, let's take a moment to review the roles and responsibilities of the organizations that support the NISP.

Recall that the DoD is the largest Cognizant Security Agency, or CSA, and has designated DSS, as its Cognizant Security Office, or CSO. As CSO, administration of the NISP is key to the overall DSS mission, and much of that administration is carried out by the DSS Industrial Security Field Operations, or ISFO. ISFO provides oversight and conducts Security Vulnerability Assessments, or SVAs, for over 13,500 cleared contractor facilities.

ISFO maintains Industrial Security Field Offices throughout the country. Field offices are grouped into four geographic regions. Each region is led by a regional director, who oversees the operation of field offices located throughout his or her region.

Each Field Office is locally managed by a Field Office Chief, or FOC, and staffed by Industrial Security Representatives, or IS Reps. The FOC assigns an IS Rep to each contractor facility.

ISFO Headquarters Functions

In addition to overseeing the field offices and their operations, ISFO oversees several DSS headquarters components including the Facility Clearance Branch, or FCB, which processes companies for Facility Clearances, or FCLs, issues FCLs, and monitors companies that hold FCLs.

ISFO also oversees the Personnel Security Management Office for Industry, or PSMO-I, which processes PCLS and monitors personnel security eligibility and access for contractors.

Finally, ISFO oversees the NISP Authorization Office, or NAO. NAO carries out DSS Assessment and Authorization, or A&A, determinations for contractor Information Systems, or ISs, to process classified information.

To learn more about each of these headquarters components, see the DSS ISFO website. Select VIEW to access this website from a list of Course Resources.

Government Roles

Overview of DSS Roles

DSS provides security support to a large number of military services, defense agencies, non-DoD Federal Agencies, and cleared contactor facilities. To do this, it relies on individuals in a variety of roles.

IS Reps serve as the contractor's primary point of contact for security matters and are responsible for contractor oversight in the NISP. There are over 200 IS Reps located throughout the country.

The Information System Security Professional/Security Control Assessor, or ISSP/SCA works with IS Reps and contractor personnel on all matters related to the authorization and maintenance of authorized contractor ISs.

Finally, Counterintelligence Special Agents, or CISAs, provide advice, oversight, and training regarding Counterintelligence, or CI, issues.

Let's review each of these roles in greater detail.

IS Rep

Industrial Security Representatives (IS Reps) serve as the contractor's primary point of contact for security matters. They work closely with the contractor's FSO, to provide advice, assistance, and oversight.

IS Reps conduct SVAs to ensure the program is in compliance with the NISPOM and receive change conditions and suspicious contact reports from the FSO.

IS Reps also receive reports of security violations, conduct administrative inquiries when appropriate, and report security violations to the GCA.

Finally, IS Reps coordinate with other entities within DSS to oversee all aspects of a contractor's Industrial Security Program, including:

- International operations
- Personnel security
- Counterintelligence/Insider threat
- Authorized Information Systems
- Special programs (e.g., Special Access Programs (SAP); Arms, Ammunition, and Explosives (AA&E))

ISSP/SCA

ISSPs/SCAs work closely with IS Reps and contractor personnel on all matters related to the authorization and maintenance of authorized contractor classified ISs.

ISSP/SCAs perform classified IS assessments and make recommendations to the Authorizing Official, or AO, and/or the Authorizing Official's Designated Representative, or AODR, the authorities who make classified IS authorization decisions.

ISSP/SCAs participate in SVAs, during which they evaluate vulnerabilities, identify potential cyber security threats, and help develop mitigation strategies. ISSP/SCAs also respond to security violations involving authorized classified ISs.

ISSP/SCAs must develop and maintain technical proficiency amidst ever changing technological developments.

CISA

CISAs provide advice, oversight, and training regarding counterintelligence issues and work with contractors to identify potential threats to U.S. technology, including insider threats.

They develop employee counterintelligence awareness and emphasize the need for reporting, and assist with foreign travel briefings and debriefings.

CISAs work with IS Reps to provide advice, assistance, and guidance as needed, specifically regarding counterintelligence best practices. CISAs also assist IS Reps in conducting SVAs.

More counterintelligence resources are available from the course resource page, http://www.cdse.edu/catalog/elearning/IS011-resources.html.

Installation Commander/Agency Head

Contractors working on government sites will also work with the installation commander or agency head.

The installation commander or agency head serves as the CSO for government-controlled and –leased facilities. They have overall responsibility for the security of the installation, including: law enforcement, traffic regulation, physical security, information security, and Information Systems security.

Installation commanders or agency heads must review and update installation directives to reflect minimum NISPOM guidance for those contractors who are required to work on the installation.

Industry Roles

Overview of Industry Roles

At contractor facilities, there are three primary roles responsible for NISP oversight.

The FSO, who effectively manages the day-to-day operation of the contractor's security program, the Information System Security Manager, or ISSM, who is responsible for managing IS security, and the Insider Threat Program Senior Official, or ITPSO, who is responsible for establishing and executing an Insider Threat Program.

The FSO may also serve as the ISSM and the ITPSO, and all of these roles must be filled in order for the facility to work on a classified contract.

Let's review these roles in greater detail.

FSO

The FSO has ultimate responsibility for the administration, oversight, and day-to-day operation of the contractor security program. These responsibilities include, but are not limited to: maintaining FCLs, initiating and maintaining PCLS, providing security education, safeguarding classified information, reporting to the government, and conducting self-inspections.

The FSO must ensure the security program meets the requirements specified in the NISPOM and in contract-specific documents such as forms DD 441 and DD 254.

The FSO works with DSS to maintain a viable security program. Specifically, they must monitor authorized classified ISs, storage, processing, and removal of classified; maintain procedures for incoming and outgoing classified visits; and educate all cleared and non-cleared* personnel on their security responsibilities.

**Note: recommended but not required*

The FSO must be a U.S. citizen employee who is cleared in connection with, and at the same classification level as, the FCL.

You can learn more about the FSO's role and responsibilities through these courses and curricula, available through the Center for Development of Security Excellence, or CDSE:

- *FSO Role in the NISP* course
- *You're a New FSO: Now What?* Short
- *FSO Program Management for Possessing Facilities* curriculum
- *FSO Orientation for Non-Possessing Facilities* curriculum
- *Insider Threat* curriculum

ISSM

An Information System Security Manager (ISSM) must be appointed by the contractor when there is a contractor-owned classified IS, or a government-owned classified IS at a contractor facility.

The ISSM works very closely with the FSO to manage each IS and ensure that IS security requirements are met. The ISSM is responsible for: implementing NISPOM IS security requirements; establishing, documenting, maintaining, and monitoring IS security programs and procedures; conducting IS security education and training; identifying and documenting unique local IS threats and vulnerabilities; notifying the CSO of relevant changes to Information Systems; and carrying out periodic self-inspections of Information Systems.

The ISSM develops facility procedures for: handling media and equipment containing classified information, implementing security features, incident reporting, user acknowledgment of responsibility, and threat detection, including auditing and monitoring for malware attacks, phishing attempts, and other threats.

More information about the ISSM's role and responsibilities can be found in several training options available through CDSE.

ITPSO

The Insider Threat Program Senior Official (ITPSO) is designated by the company and must be a U.S. citizen employee who is cleared in connection with, and at the same classification level as, the FCL. The ITPSO is responsible for establishing and maintaining an Insider Threat Program that gathers, integrates, and reports any information that might indicate an insider threat.

If the ITPSO and FSO roles are filled by different individuals, the ITPSO must make sure that the FSO is an integral member of the insider threat program.

Lesson 3 Review Activities

Review Activity 1

Contractor CEO: Which roles will we need to fill at our company, and which are government roles?

Identify whether the following roles are filled by government or industry employees. Check your answer in the Answer Key at the end of this Student Guide.

Facility Security Officer (FSO)

- ○ Government
- ○ Industry

Information System Security Professional/Security Control Assessor (ISSP/SCA)

- ○ Government
- ○ Industry

Information System Security Manager (ISSM)

- ○ Government
- ○ Industry

Industrial Security Representative (IS Rep)

- ○ Government
- ○ Industry

Counterintelligence Special Agent (CISA)

- ○ Government
- ○ Industry

Insider Threat Program Senior Official (ITPSO)

- ○ Government
- ○ Industry

Review Activity 2

Contractor CEO: And what do each of these individuals do?

Identify the role described by each statement. Check your answer in the Answer Key at the end of this Student Guide.

This DSS employee serves as the contractor's primary point of contact for security.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

This DSS employee oversees authorized contractor Information System use.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

This contractor employee administers and oversees the contractor security program.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

This contractor employee manages Information Systems and ensures Information System security requirements are met.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

This contractor employee establishes and maintains the insider threat program.

- Information System Security Professional/Security Control Assessor (ISSP/SCA)
- Facility Security Officer (FSO)
- Insider Threat Program Senior Official (ITPSO)
- Information System Security Manager (ISSM)
- Industrial Security Representative (IS Rep)

Lesson 4: Contracting Process in the NISP

Introduction

Objectives

Prime Contractor FSO: I know you already have a classified contract in place, but I think it would be helpful for you to know how the general contracting process works.

Subcontractor CEO: Good idea - even though we have been awarded our first classified contract, I'm sure there's still a lot to learn.

Main Narrator: Because industrial security involves both the government and industry working closely together, it is important that both parties verify, document, and understand their contractual requirements. This will ensure everyone involved successfully performs and accomplishes their respective contractual responsibilities.

Here are the lesson objectives. Take a moment to review them.

- Identify the essential steps of the NISP contracting process
- Recognize key roles associated with the NISP contracting process
- Indicate the purpose of several NISP contracting documents, including the Statement of Work (SOW), DD Form 254, and DD Form 441

The Contracting Process

Contracting Process Overview

The contracting process begins when the government identifies the need for a service or product. The Government Contracting Activity, or GCA, defines the initial requirements for the product or service, as well as the acquisition strategy for the contract. This strategy includes a list of the final contract deliverables, how those deliverables are defined, and the options, if any.

Next, the GCA publishes a Request for Proposal, or RFP, as part of the solicitation stage. The RFP includes the contract requirements, including the contract clause, work statements, specifications, delivery schedule, and payment terms. Contractors who meet the qualifications of the RFP respond with a written proposal. The GCA evaluates the submitted proposals and, based on the criteria outlined in the GCA's RFP, awards the contract to the contractor that provides the best value to the government.

Once the contract is awarded, the cleared contractor performs the work, adhering to all provisions of the classified contract.

Classified Contract Details

A classified contract requires a few additional considerations.

The government must verify that the contractor has a valid Facility Clearance, or FCL, at the appropriate level, and, if applicable, appropriate storage capabilities. If the company does not have a valid FCL, the government will need to sponsor the company for an initial FCL at the proper level. If the company has an FCL at a lower level than required by the contract, the government will need to sponsor an upgrade to the proper level prior to awarding any classified contracts.

After a classified contract is awarded, the GCA must issue the required contractual security documentation in accordance with the industrial security provisions necessary for the task, including a clause that requires the contractor to follow the provisions of the NISPOM. The contract must also include a DD Form 254, Department of Defense Contract Security Classification Specification, which will provide security requirements and classification guidance.

Contracting and the Acquisition Lifecycle

The contracting process you just saw is just one part of the DoD acquisition life cycle, in which a new product or technology is taken from initial need identification, through Materiel Solution Analysis, or MSA, Technology Maturation and Risk Reduction, or TMRR, Engineering and Manufacturing Development, or EMD, Production and Deployment, or P&D, and Operations and Support, or O&S.

Throughout the DoD acquisition life cycle, multiple contract awards can occur, and each of these will follow the contracting process we just reviewed.

For more information on acquisitions and contracting as they relate to the NISP, refer to the glossary and to the Acquisition and Contracting Basics in the NISP course available through the Center for Development of Security Excellence, or CDSE.

Contracting Officials

Contract administration involves two primary government employees: the Contracting Officer, or CO, and the Contracting Officer's Representative, or COR.

Contracting Officer

The Contracting Officer, or CO, is a government employee with the authority to enter into, administer, and terminate contracts. Note that although the acronym CO is frequently used, some military installations may use a different acronym, such as KO, to avoid confusion with "Commanding Officer."

The Contracting Officer typically has oversight and contract responsibility for numerous programs, although he or she may delegate authority for contract administration to an

Administrative Contracting Officer, or ACO. Authority for settling terminated contracts may be delegated to a Termination Contracting Officer, or TCO.

Contracting Officer's Representative

The COR is a government employee designated by the CO. CORs are assigned to specific contracts, and oversee the contracting process, making sure that all of the necessary requirements are met. For each contract, CORs determine whether a contractor has the need for access to classified information, verify the contractor's FCL, and sponsor the contractor for an FCL if necessary.

CORs stay in close contact with the contractor and serve as Subject Matter Experts, or SMEs, for the project. They communicate the security requirements and classification guidance from the procurement process through contract completion, and they closely monitor contractor performance.

Note that the COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract; these are the responsibility of the CO.

Contract Documentation

Documentation Overview

Classified contracts for goods or services include security clauses, as required by the Federal Acquisition Regulation, or FAR and the Defense Federal Acquisition Regulation Supplement, or DFAR.

Contractors must follow all security classification guidance provided in their classified contract and all security requirements must be addressed in the contract, including rules for Controlled Unclassified Information, or CUI, such as Personally Identifiable Information, or PII.

Several key contract documents outline these responsibilities and requirements, including the Statement Of Work, or SOW, DD Form 254, the DoD Contract Security Classification Specification, and DD Form 441, the DoD Security Agreement.

Statement of Work

The first document you should be familiar with is the SOW. In the SOW, the government provides the contractor with key background information and explains the objective and completion of the desired end product.

The SOW contains contract information including: project scope, deadlines, and steps; contractor details such as lists of contract working personnel, billing hours, and rates; clearance levels required; and travel, if applicable.

DD Form 254

The Department of Defense Contract Security Classification Specification, commonly referred to as DD Form 254, is one of the most important contract forms you will use.

DD Form 254 is required for all contracts requiring access to classified information, as specified in the Federal Acquisition Regulation, Subpart 504.4. It provides contractors with the security requirements and security classification guidance needed to perform on the classified contract, including specific clearance and access requirements, authorization to generate classified information, classified storage requirements, instructions about public disclosure, and any other special security regulations above and beyond those detailed in the NISPOM.

To ensure that appropriate guidance is provided to the contractor, it is recommended that the execution of the DD Form 254 be a collaborative effort between someone with contracting authority and knowledge – for example the COR, someone with program knowledge and subject matter expertise, like the program manager for the contract, and someone who understands information and industrial security requirements, like the FSO or security specialist.

The following Job Aids containing more information and completion guidance for the DD Form 254 are available from CDSE:

- DD Form 254: Enhanced DD Form 254 with information pop-ups, dropdowns and an Item 13 continuation page https://stepp.dss.mil/courseware/dd254/ddform254fillable.pdf
- DD Form 254: A Guide for the Preparation of a DD Form 254 (http://www.cdse.edu/documents/cdse/DD254.pdf)

DD Form 441

Finally the DoD Security Agreement, or DD Form 441, is a legally binding contract between the U.S. Government and the contractor. The DD Form 441 is executed when a company receives its FCL and must be completed before any work on a classified contract begins.

By signing this security agreement, the contractor makes a commitment to implement and maintain a system of security controls within the company in accordance with the requirements found in the NISPOM, including immediate compliance with any NISPOM modifications. The contractor also agrees to determine that any subcontractor that will involve access to classified information has been granted an appropriate FCL. Finally, the contractor acknowledges the government's authority to review the contractor's security program to ensure compliance.

By signing the agreement, the government makes a commitment to process PCLs for contractor employees as appropriate and agrees to provide security classification guidance and oversight.

Lesson 4 Review Activities

Review Activity 1

Contractor CEO: Which comes first in the contracting process?

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

What is the first step of the contracting process?

- ○ The GCA defines the acquisition strategy for the contract.
- ○ The GCA publishes a Request for Proposal (RFP).
- ○ The government identifies a need for a product or service.
- ○ The GCA defines the initial requirements for the product/service.

Review Activity 2

Contractor CEO: We worked with both the CO and the COR during the contracting process, but I could use a refresher. Who does what?

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

Who has authority to enter into, administer, and terminate contracts?

- ○ Contracting Officer (CO)
- ○ Contracting Officer's Representative (COR)

Who serves as Subject Matter Expert (SME) for individual contracts?

- ○ Contracting Officer (CO)
- ○ Contracting Officer's Representative (COR)

Who provides contractual oversight and has responsibility for multiple programs?

- ○ Contracting Officer (CO)
- ○ Contracting Officer's Representative (COR)

Who closely monitors contractor performance on individual contracts?

- ○ Contracting Officer (CO)
- ○ Contracting Officer's Representative (COR)

Review Activity 3

Contractor CEO: Moving forward, where do I turn to find important contract information?

Identify which document contains the information described. Check your answer in the Answer Key at the end of this Student Guide.

Security requirements and classification guidance:

- ○ Statement of Work (SOW)
- ○ DD Form 254: DoD Contract Security Classification Specification (DD 254)
- ○ DD Form 441: DoD Security Agreement (DD 441)

Contract details such as project scope, deadlines, and steps:

- ○ Statement of Work (SOW)
- ○ DD Form 254: DoD Contract Security Classification Specification (DD 254)
- ○ DD Form 441: DoD Security Agreement (DD 441)

A security agreement between a contractor and the DoD in order to prevent the unauthorized disclosure of classified information:

- ○ Statement of Work (SOW)
- ○ DD Form 254: DoD Contract Security Classification Specification (DD 254)
- ○ DD Form 441: DoD Security Agreement (DD 441)

Lesson 5: Clearance Requirements in the NISP

Introduction

Objectives

Subcontractor CEO: So, our employees working on the classified contract need to be cleared, right?

Prime Contractor FSO: Yes, your employees working on that classified program will need a valid PCL, just like your company needed a valid FCL before it was awarded its classified contract.

Main Narrator: Before the government entrusts classified information to cleared companies and their employees, it must ensure that organizations are free from conflicts of interest, are responsible, and that individuals within their organization are loyal, trustworthy, and reliable.

Here are the lesson objectives. Take a moment to review them.

- Explain the purpose of Facility Clearances (FCLs)
- Recall the process of obtaining an FCL
- Describe requirements for obtaining a Personnel Security Clearance (PCL)
- Recall the process of obtaining a PCL
- Explain the process of terminating a PCL
- Outline the procedures for hosting classified visits

Facility Clearances

What is an FCL?

In order to access classified information in the performance of a classified contract, a company must first have an appropriate Facility Clearance, or FCL, and if required, applicable safeguarding. The FCL is an administrative determination that a company is eligible for access to classified information of a certain classification level and all lower levels.

Approved safeguarding allows the storage of classified information within the facility at the same classification level as the company's FCL, or lower.

Note that a contractor or facility cannot access or possess classified material until the FCL is granted and safeguarding capabilities are approved by DSS; just because a company is cleared does not mean they can store, receive, or generate classified information.

When a company receives an FCL, it is not the actual facility building or structure that is cleared, but the individuals who run, own, and manage the facility. The FCL is contingent upon all Key Management Personnel, or KMP, being granted a Personnel Security Clearance, or PCL. These KMP must be cleared before the FCL will be granted.

Obtaining an FCL

Recall that the Facility Clearance Branch, or FCB, is the Defense Security Service, or DSS, office that processes and issues FCLs. To do this, it reviews the facility's sponsorship, which was received from either another cleared company or a government agency; the security agreement; any Foreign Ownership, Control, or Influence, or FOCI, issues; as well as the facility's business structure and organization. It ensures that the appropriate KMP are identified and properly cleared.

Once the FCL is granted, employees who need to access classified information, whether at their contractor facility, at another cleared facility, or at a government installation, may be processed for their PCL.

You can learn more about facility clearances through these courses, available through CDSE:

- *Facility Clearances in the NISP* course
- *Business Structures in the NISP* course
- *KMP: To Clear or Not to Clear* short

Personnel Security Clearances

Eligibility and Access

Before employees begin the PCL process, the contractor must determine which employees will be working on the classified contract and will require access to classified information. If a determination is made that there is a requirement for access to classified information, a PCL is required.

The process for an initial PCL includes completion of the appropriate national security investigation and a favorable eligibility determination. In order to have access to classified information, the individual must have a favorable clearance eligibility determination at the proper level, possess a need-to-know, and execute a Classified Information Non-Disclosure Agreement, or SF 312. It is important to note, however, that just because an individual is granted a PCL does not mean he or she may have access to all classified information.

Individuals must have a specific Need-To-Know, or NTK, for the classified information they will access. For more information, see the Need-to-Know Video available through CDSE.

PCL Process

The initial determination that an employee requires a PCL is generally made by the program manager. The program manager considers whether the employee requires access to classified information in the performance of a classified contract. The program manager determines need only; he or she does not approve the clearance level. The clearance level is determined by the GCA as stated in the RFP.

Once the employee's need for a PCL is established, the Facility Security Officer, or FSO, initiates the process and instructs the employee to complete the Standard Form 86, or SF-86, also known as the Questionnaire for National Security Positions. Employees complete the SF-86 electronically using software provided by the investigative agency.

Next, the FSO sends the completed SF-86 to the Personnel Security Management Office for Industry, or PSMO-I, for processing. PSMO-I determines whether the request for a clearance is legitimate and, if so, forwards the application to the investigative agency that will conduct the background investigation.

The investigative agency puts all of the information collected into a report that the DoD Consolidated Adjudications Facility, or DoD CAF, reviews. The DoD CAF uses the national standards laid out in the DoDM 5200.2, Procedures for the DoD Personnel Security Program, to make a national security eligibility determination. If the determination is favorable, the DoD CAF records the eligibility level in the DoD system of record.

Based on need, the FSO may then grant the employee access to classified information, up to the level for which the employee is eligible.

You can learn more about PCLs in these courses, available through CDSE:

- *Personnel Clearances in the NISP* course
- *Introduction to Personnel Security* course
- *Clearances in Industrial Security, Putting it All Together* course

Terminating Access

It is likely that an individual's access requirements may change several times over the course of their career. The government requires continued evaluation of the need for a PCL. When access is no longer needed, the FSO must "debrief" or remove the employee's access in the current DoD system of record. Eligibility remains in the system of record even when access is terminated by the FSO.

Additionally, the FSO must debrief employees who no longer require access and remove their names from any access rosters and/or any active Visit Authorization Letters, or VALs, on which they may be included.

Visits

Visit Procedures

Procedures for hosting classified visits vary from one facility or installation to another. In general, the party who is disclosing the classified information is responsible for ensuring that visitors are authorized persons with the appropriate PCL and NTK. Remember, NTK is determined based on the person's professional and contractual duties.

Contractors are responsible for supplying their employee's clearance information to the host facility prior to the visit through the current DoD system of record, or if that is not available, with a VAL.

Cleared personnel from contractors who are visiting another cleared facility or a government installation, regardless of the length of their visit, must follow the security requirements of the host activity.

For more information, refer to the *Visits and Meetings in the NISP* course, from CDSE.

When a visit requires access to classified information, the host contractor must verify the visitor's PCL level. Verification of a visitor's PCL may be accomplished by a review of a CSA designated database that contains the information or by a visit authorization letter (VAL) provided by the visitor's employer.

If a VAL is required, contractors must include the following information:

1. Contractor's name, address, and telephone number, assigned Commercial and Government Entity (CAGE) code, if applicable, and certification of the level of the facility security clearance
2. Name, date and place of birth, and citizenship of the employee intending to visit
3. Certification of the proposed visitor's PCL and any special access authorizations required for the visit
4. Name of person(s) to be visited
5. Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit
6. Date or period during which the VAL is to be valid

Lesson 5 Review Activities

Review Activity 1

Contractor CEO: I may still have some misconceptions about clearance requirements. Can you tell me if I have the following information correct?

Determine whether each statement is true or false. Check your answer in the Answer Key at the end of this Student Guide.

Once the company's FCL is in place, contractors may begin to access classified materials.

- ○ True
- ○ False

Key Management Personnel must be cleared before the FCL will be granted.

- ○ True
- ○ False

An employee's approved national security eligibility determination, or PCL, is the same as his/her access.

- ○ True
- ○ False

Review Activity 2

Could you help me review the steps of the PCL process? What has to happen first?

Determine the correct order of the steps of the PCL process. Check your answer in the Answer Key at the end of this Student Guide.

What is the first step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

What is the second step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

What is the third step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

What is the fourth step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

What is the fifth step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

What is the sixth step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I approves request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

Lesson 6: Course Conclusion

Conclusion

Course Summary

Subcontractor CEO: Well, thanks for all of your help. Even though we still have a lot to do – and a lot to learn – we now know our next steps and the many resources that are available.

Contractor- FSO: You're welcome. And remember we are here to support you and your company moving forward.

Main Narrator: In this course you reviewed the purpose and structure of the National Industrial Security Program, or NISP, key security roles in both government and industry, the general contracting process for classified contracts, and clearance requirements in the NISP.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Overview of the NISP
- Security Roles in the NISP
- Contracting Process in the NISP
- Clearance Requirements in the NISP
- Course Conclusion

Lesson Summary

Congratulations! You have completed the *Introduction to Industrial Security* course.

You should now be able to perform all of the listed activities.

- Recognize the role of the National Industrial Security Program (NISP) in the protection of classified information entrusted to industry
- Describe government and contractor security roles and responsibilities in accordance with the NISP Operating Manual (NISPOM)
- Outline the process and requirements for establishing a classified contract
- Identify the security clearance processes and procedures required for access to classified information

To receive course credit, you must take the *Introduction to Industrial Security* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

Contractor CEO: My company, BuildGen Contracting, just won its first classified government contract. What are our NISP responsibilities?

What are contractor responsibilities according to the NISP?

Select the best response.

- ○ Establish NISP requirements for the protection of classified information
- ○ Provide advice, assistance, and oversight
- ⊙ Implement NISP requirements for the protection of classified information (correct response)

***Feedback**: Contractors must implement all NISP requirements in order to ensure classified information is protected. The government is responsible for establishing requirements and providing advice, assistance, and oversight.*

Review Activity 2

Contractor CEO: Can you help me understand what the difference is between CSAs and CSOs?

Identify whether the following statements describe CSAs or CSOs.

These organizations establish industrial security programs and oversee security requirements.

- ⊙ CSA (correct response)
- ○ CSO

***Feedback:** CSAs establish industrial security programs and oversee security requirements.*

These organizations administer the NISP and provide security guidance, oversight, and policy clarifications.

- ○ CSA
- ⊙ CSO (correct response)

***Feedback**: CSOs administer the NISP and provide security guidance, oversight, and policy clarifications.*

Review Activity 3

Contractor CEO: I understand DSS will be the CSO for our company. What will they do for us?

Which of these are DSS responsibilities or functions?

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

- ☑ Provide security guidance and oversight (correct response)
- ☑ Provide policy clarifications (correct response)
- ☑ Conduct Security Vulnerability Assessments (SVAs) (correct response)
- ☐ Provide installation-specific procedures for work performed on a government installation
- ☐ Provide contract-specific security classification guidance

***Feedback**: DSS provides security guidance and oversight and policy clarifications, and conducts Security Vulnerability Assessments (SVAs). Installation commanders provide installation-specific procedures for work performed on a government installation, and GCAs provide contract-specific security classification guidance.*

Lesson 3 Review Activities

Review Activity 1

Contractor CEO: Which roles will we need to fill at our company, and which are government roles?

Identify whether the following roles are filled by government or industry employees.

Facility Security Officer (FSO)

- ○ Government
- ⦿ Industry (correct response)

***Feedback**: FSO is an industry role.*

Information System Security Professional/Security Control Assessor (ISSP/SCA)

- ⦿ Government (correct response)
- ○ Industry

***Feedback**: ISSP/SCA is a government role.*

Information System Security Manager (ISSM)

- ○ Government
- ⦿ Industry (correct response)

***Feedback**: ISSM is an industry role.*

Industrial Security Representative (IS Rep)

- ⦿ Government (correct response)
- ○ Industry

***Feedback**: IS Rep is a government role.*

Counterintelligence Special Agent (CISA)

- ⦿ Government (correct response)
- ○ Industry

***Feedback**: CISA is a government role.*

Insider Threat Program Senior Official (ITPSO)

- ○ Government
- ⦿ Industry (correct response)

***Feedback**: ITPSO is an industry role.*

Review Activity 2

And what do each of these individuals do?

Identify the role described by each statement.

This DSS employee serves as the contractor's primary point of contact for security.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ⊙ Industrial Security Representative (IS Rep) (correct response)

***Feedback:** IS Reps serve as the contractor's primary point of contact for security.*

This DSS employee oversees authorized contractor Information System use.

- ⊙ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

***Feedback:** ISSP/SCAs oversee authorized contractor Information System use.*

This contractor employee administers and oversees the contractor security program.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ⊙ Facility Security Officer (FSO) (correct response)
- ○ Insider Threat Program Senior Official (ITPSO)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

***Feedback:** FSOs administer and oversee contractor security programs.*

This contractor employee manages Information Systems and ensures Information System security requirements are met.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)

- ○ Insider Threat Program Senior Official (ITPSO)
- ⦿ Information System Security Manager (ISSM) (correct response)
- ○ Industrial Security Representative (IS Rep)

Feedback: *ISSMs manage Information Systems and ensure Information System security requirements are met.*

This contractor employee establishes and maintains the insider threat program.

- ○ Information System Security Professional/Security Control Assessor (ISSP/SCA)
- ○ Facility Security Officer (FSO)
- ⦿ Insider Threat Program Senior Official (ITPSO) (correct response)
- ○ Information System Security Manager (ISSM)
- ○ Industrial Security Representative (IS Rep)

Feedback: *ITPSOs establish and maintain contractor insider threat programs.*

Lesson 4 Review Activities

Review Activity 1

Contractor CEO: Which comes first in the contracting process?

Select the best response.

What is the first step of the contracting process?

- ○ The GCA defines the acquisition strategy for the contract.
- ○ The GCA publishes a Request for Proposal (RFP).
- ⊙ The government identifies a need for a product or service. (correct response)
- ○ The GCA defines the initial requirements for the product/service.

Feedback: *Before anything else happens, to initiate the contracting process the government must identify the need for a product or service.*

Review Activity 2

Contractor CEO: We worked with both the CO and the COR during the contracting process, but I could use a refresher. Who does what?

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

Who has authority to enter into, administer, and terminate contracts?

- ⊙ Contracting Officer (CO) (correct response)
- ○ Contracting Officer's Representative (COR)

Feedback: *The CO has the authority to enter into, administer, and terminate contracts. Who serves as Subject Matter Expert (SME) for individual contracts?*

- ○ Contracting Officer (CO)
- ⊙ Contracting Officer's Representative (COR) (correct response)

Feedback: *The COR serves as Subject Matter Expert (SME) for individual contracts.*

Who provides contractual oversight and has responsibility for multiple programs?

- ⊙ Contracting Officer (CO) (correct response)
- ○ Contracting Officer's Representative (COR)

Feedback: *The CO provides contractual oversight and has responsibility for multiple programs.*

Who closely monitors contractor performance on individual contracts?

- ○ Contracting Officer (CO)
- ⊙ Contracting Officer's Representative (COR) (correct response)

Feedback: *The COR closely monitors contractor performance on individual contracts.*

Review Activity 3

Contractor CEO: Moving forward, where do I turn to find important contract information?

Identify which document contains the information described.

Security requirements and classification guidance:

- ○ Statement of Work (SOW)
- ⊙ DD Form 254: DoD Contract Security Classification Specification (DD 254) (correct response)
- ○ DD Form 441: DoD Security Agreement (DD 441)

Feedback: *DD Form 254 contains security requirements and classification guidance. Note: the SOW may also contain this information.*

Contract details such as project scope, deadlines, and steps:

- ⊙ Statement of Work (SOW) (correct response)
- ○ DD Form 254: DoD Contract Security Classification Specification (DD 254)
- ○ DD Form 441: DoD Security Agreement (DD 441)

Feedback: *SOW contains contract details such as project scope, deadlines, and steps.*

A security agreement between a contractor and the DoD in order to prevent the unauthorized disclosure of classified information:

- ○ Statement of Work (SOW)
- ○ DD Form 254: DoD Contract Security Classification Specification (DD 254)
- ⊙ DD Form 441: DoD Security Agreement (DD 441) (correct response)

Feedback: *DD Form 441 is a legally binding contract document and serves as a record of the contractor's commitment to comply with the NISPOM.*

Lesson 5 Review Activities

Review Activity 1

Contractor CEO: I may still have some misconceptions about clearance requirements. Can you tell me if I have the following information correct?

Determine whether each statement is true or false.

Once the company's FCL is in place, contractors may begin to access classified materials.

- ○ True
- ⊙ False (correct response)

Feedback: *Contractors may not access classified information without approved national security eligibility determinations, or PCLs. The company submits employee PCL requests after the FCL has been approved.*

Key Management Personnel must be cleared before the FCL will be granted.

- ⊙ True (correct response)
- ○ False

Feedback: *Key Management Personnel must be cleared before the FCL will be granted.*

An employee's approved national security eligibility determination, or PCL, is the same as his/her access.

- ○ True
- ⊙ False (correct response)

Feedback: *An employee's national security eligibility determination, or PCL, does NOT on its own grant access to classified information. An individual must have a PCL at the appropriate level, a Need-To-Know for the specific classified information, and have executed a SF-312, Classified Information Non-Disclosure Agreement (NDA).*

Review Activity 2

Could you help me review the steps of the PCL process? What has to happen first?

Determine the correct order of the steps of the PCL process.

What is the first step of the PCL process?

- ○ Employee completes SF-86
- ⦿ Program Manager determines need for access(correct response)
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

Feedback: *First, the Program Manager determines the employee's need for classified access.*

What is the second step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ⦿ FSO initiates PCL process (correct response)

Feedback: *Next, the FSO initiates the PCL process.*

What is the third step of the PCL process?

- ⦿ Employee completes SF-86 (correct response)
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

Feedback: *Next, the employee completes the SF-86.*

What is the fourth step of the PCL process?

- ○ Employee completes SF-86

- ○ Program Manager determines need for access
- ⦿ PMSO-I validates the request (correct response)
- ○ Investigative agency conducts investigation
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

Feedback: *Next, the PSMO-I determines that the PCL request is legitimate.*

What is the fifth step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ⦿ Investigative agency conducts investigation (correct response)
- ○ DoD CAF grants and records PCL
- ○ FSO initiates PCL process

Feedback: *Next, the investigative agency conducts background investigation.*

What is the sixth step of the PCL process?

- ○ Employee completes SF-86
- ○ Program Manager determines need for access
- ○ PMSO-I validates the request
- ○ Investigative agency conducts investigation
- ⦿ DoD CAF grants and records PCL (correct response)
- ○ FSO initiates PCL process

Feedback: *Finally, the DoD CAF makes a determination to grant or not grant the PCL and records the eligibility determination in the DoD system of record.*