Student Guide

Course: Introduction to Industrial Security

Lesson1: Introduction and Purpose

Lesson Introduction

Welcome. In this lesson, you will be introduced to the purpose of the Industrial Security Program. During the time we spend in this lesson, we are going to take a look at the purpose of the National Industrial Security Program, also called the NISP, which establishes standards for contractors who have access to classified information. We will also look at a few security requirements for contractors in different environments.

Here's a fact to consider. Much of all U.S. classified information originates within the industrial environment. Every day, contractors have access to our classified and unclassified sensitive information, as well as to our 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.

Contractors in the DoD Security Environment

1. Purpose of the NISP

The National Industrial Security Program, also called the NISP, was established in 1993 by Executive Order 12829. The goal of the NISP is to safeguard classified information that is in the possession of government contractors, licensees, or grantees in the most efficient and cost effective manner possible. The NISP applies to all executive branch departments and agencies. The purpose of the NISP is to define the requirements, restrictions, and other safeguards in order to prevent unauthorized disclosure of classified information.

The NISP operating manual is DoD 5220.22-M, which is more commonly referred to as the NISPOM, or the National Industrial Security Program Operating Manual. Achieving greater uniformity in security requirements is essential to the safeguarding of all sensitive and classified information between the government and industry. Through the NISP this goal is being achieved.

2. Security Requirements on Unclassified Contracts

There may be times when a company or individual has a contract with the government to conduct work that is unclassified. Even in these cases, there are still security requirements that must be addressed. This section covers some of those requirements.

Contractor employees are often exposed to unclassified sensitive information that requires some level of protection. Examples of sensitive information may include budget and financial information, personal information, or specific procedures. Contractor

employees who have access to government-owned information systems must be vetted based on the sensitivity of the system, and their duties and privileges within that system. In some cases, contractor employees have access to military installations, government office space, or other sensitive areas, and may also be subject to some type of vetting.

When security requirements such as these or others exist, they must be written into requests for proposals and contracts. The contract language must be specific enough to identify what the security requirement is, and how the contractor will be reimbursed for costs associated with the requirement.

3. Contractors Working on Government Installations

When the government issues a request for proposal, they can determine that the work be performed on the contractor's facility, or it may be executed on the government site. Either way, there are guidelines and procedures that must be adhered to pertaining to security. In this section, we are going to focus on what may be expected of a contractor who is working on a government installation, though not necessarily within a classified workspace.

When contractors are working on a government installation, the contract should contain provisions obligating them to follow the established procedures of the installation. The installation procedures may include undergoing a cursory background check to enter the installation without an escort, providing personal vehicle and insurance information to obtain a vehicle pass, or if the individual will be working with an information system, they may have to undergo a background investigation. All of these are examples of what may be required of a contractor working on a government installation. Each applicable requirement must be addressed in the contract.

4. Contractors Working at Their Own Facility

As we just learned, when contractors work at a government facility, they follow the security requirements of the facility. These rules are typically established by the installation commander, unless there is another appointed cognizant authority. When contractors work at their own facility, the rules are a little different.

If a contractor has a cleared facility and processes classified information at that facility, the contractor is required to follow procedures that are provided in the NISP Operating Manual, also known as the NISPOM. In some cases, additional security requirements appear in the contract. The contractor's involvement in the NISP is overseen by a cognizant security office. The Defense Security Service, also known as DSS, is the cognizant security office for most classified Department of Defense contracts.

Cleared contractors working at their own facility can expect periodic reviews from their cognizant security office to ensure that the NISPOM and contract guidelines are being followed. During a review, the Industrial Security Representative will evaluate the effectiveness of the facility's security program, including all requirements of the NISPOM. Some of the things they may look at include how classified information is stored, visit procedures, security awareness and training, procedures for protecting classified information on information systems, eligibility for access of individuals working

on classified information, and the company's records to identify any changes in ownership, management, or foreign involvement since the last review.

In summary, they review the facility's security program to ensure compliance with applicable guidance.

Lesson Summary

Contractors who support the Department of Defense are subject to various security requirements. These requirements come from national policy, DoD regulations, and local implementing procedures. When one stops to consider the significant amount of classified information generated within the industrial environment, the impact of industry on national security becomes apparent. The National Industrial Security Program is a partnership between the federal government and private industry in order to safeguard classified information.

We looked at security requirements for unclassified contracts and the procedures used to ensure the protection of sensitive or critical information. Contractors who work on a Government installation are obligated to adhere to the installation security rules and regulations, established by the commander or other appointed cognizant authority as specified in their contract. Contractors who work at their own cleared facility are overseen by a cognizant security office, which in most cases is the Defense Security Service. It is the responsibility of the cognizant security office to make sure that all of the requirements of the NISP, and other requirements outlined in the contract, are being met at the contractor's facility.

In summary, contractors are a valuable partner in national security. Security professionals should be aware that contracts, in order to be effective, must contain clear guidance on security requirements.

Review Activity

Fill in the blanks by matching each word to the sentence in which it belongs. Check your answers in the Answer Key at the end of this Student Guide.

A. NISP	__	Much of U.S. classified information originates within the _____ environment.
B. Industrial	__	If a contractor works at his/her own facility, security compliance is overseen by the _____.
C. Installation	__	When a contractor is working at a government installation, he/she must adhere to the security rules of the _____ commander.
D. Defense Security Service	__	The goal of the _____ is to safeguard classified information in the possession of the government contractors.

Answer Key

A. NISP	_B_	Much of U.S. classified information originates within the _____ environment.
B. Industrial	_D_	If a contractor works at his/her own facility, security compliance is overseen by the _____.
C. Installation	_C_	When a contractor is working at a government installation, he/she must adhere to the security rules of the _____ commander.
D. Defense Security Service	_A_	The goal of the _____ is to safeguard classified information in the possession of the government contractors.

Student Guide

Course: Introduction to Industrial Security

Lesson 2: Industrial Roles and Responsibilities

Lesson Introduction

Just as in any other security program, there are certain roles that play a very important part in making the industrial security program a success. In this lesson, we are going to take a look at some of these roles and their associated responsibilities. We will examine the roles of the Facility Security Officer, the Information Systems Security Manager, and the Industrial Security Representative of the cognizant security office.

Facility Security Officer and the IS Rep

1. FSO Responsibilities

Now let's look at the role of the Facility Security Officer, also referred to as an FSO. The FSO has the ultimate responsibility for the administration and the day-to-day operation of the security program at a cleared contractor facility. You can think of the FSO as the industry counterpart to a government employee who is a security specialist.

The major responsibilities of the FSO are ensuring compliance with the NISP and following National Industrial Security Program Operating Manual, or NISPOM, guidelines. The FSO also has a variety of other duties.

a. Ensuring Compliance with the NISP

The FSO ensures compliance with the NISP by:

- Monitoring approved classified information systems, storage, processing, and removal
- Working with DSS in maintaining a viable security program
- Maintaining procedures for incoming and outgoing classified visits
- Educating all cleared personnel on their security responsibilities

b. Following NISPOM Guidelines

The FSO is responsible for ensuring that NISPOM guidelines are met in order to remain compliant with the requirements of the DD Form 441 – DoD Security Agreement, a legally binding agreement with the government that outlines the terms for safeguarding classified information.

c. Additional FSO Duties

Additional duties of the FSO include:

- Providing oversight of all security practices at the facility
- Educating cleared individuals

2. Industrial Security Representative

An Industrial Security Representative, or IS Rep, is an employee of the Cognizant Security Office, usually the Defense Security Service. The IS Rep is a cleared contractor's primary point of contact within the government for security matters.

The IS Rep assigned to a facility works closely with the Facility Security Officer to provide advice, assistance, and oversight. The IS Rep conducts security inspections or "reviews" of the contractor's security program to ensure compliance with NISP requirements.

3. Summary

As a security professional, it is likely that you will at some point work or interact with the FSO of a cleared contractor facility. In future lessons, you will learn much more about their duties and responsibilities. For now, it is important for you to understand that an FSO's primary responsibility is to ensure that his or her cleared facility and its employees follow the provisions spelled out in the NISPOM.

Review Activity 1

Try answering the following question. Select all that apply. Check your answers in the Answer Key at the end of this Student Guide.

Which of the following are responsibilities of the FSO?

- ☐ Ensure compliance with the NISP
- ☐ Search all employees' desks regularly
- ☐ Follow NISPOM guidelines
- ☐ Guard the front entrance of the facility
- ☐ Provide training for cleared individuals

Information Systems Security

1. Information Systems

Information systems are extremely important assets which may affect national security. There is often very valuable information stored in these systems which needs to be continuously protected. The systems could be government-owned, or they could be contractor-owned. Let's look at the provisions for security of information systems accessed by contractor employees.

First, imagine a situation where a contractor employee will be given access to a government-owned computer system. The requirements for safeguarding information on the system are determined by the owner of the system. These requirements must be followed by the contractor. For example, if a contractor employee works on a military installation and has access to an information system owned by the government, he or she must follow the rules and procedures that have been established for that system.

These procedures usually include, among other things, a background investigation commensurate with the individual's duties, and the sensitivity of information on the system. The contract should contain a clause that identifies these security requirements.

Here's another scenario. If a contractor processes classified information on a company-owned information system, the provisions of Chapter 8 of the NISPOM apply. A third situation sometimes occurs; this is when a government-owned computer system is used at a contractor site. In these cases, the requirements of the NISPOM Chapter 8 take precedence over local procedures.

2. Information Systems Security Manager

In the case of a contractor-owned system or a government-owned system at a contractor facility, the facility must appoint an individual as the Information Systems Security Manager, or ISSM. The ISSM is the person within the company who is responsible for implementing NISPOM requirements related to information systems security. The ISSM and the FSO work very closely with one another, and in some cases, one person assumes both roles.

3. Summary

Protecting information systems is essential in safeguarding our nation's sensitive or classified information. Whether a contractor is working at a government site or at his or her own facility, there are always going to be security provisions to follow.

If you are working at a government site, you have to follow the security provisions that are outlined by the owner of the system. If you are working with classified information on an information system at a contactor site, you can locate the security provisions that you must follow in Chapter 8 of the NISPOM.

Review Activity 2

Try answering the following question. When you are finished, see the Answer Key at the end of this Student Guide to check your answer.

If you are a government contractor working on a contractor-owned system at a contractor facility, which security provisions must you follow?

- ☐ Chapter 8 of the NISPOM
- ☐ The government installation's regulations
- ☐ Your company's private security regulations

Contractor Compliance with Security Requirements

1. Security Requirements

Contracts for goods or services agreed upon between the customer, sometimes called the government contracting activity, and the contractor will include security clauses as

required by the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement. All security requirements must be addressed in the contract.

2. Security Procedures

When a contractor is performing work at a government facility, the contract may require him or her to adhere to the security procedures associated with that particular installation or agency. Contracts that require contractors to have access to classified information include a clause that requires the contractor to follow the provisions of the NISPOM.

3. Summary

This has been a brief introduction to how security requirements may be included in government contracts. You will learn more in future courses. The most important thing for you to know at this point is that every security requirement levied upon a contractor must be addressed in the contract. Requirements for protection of classified information at contractor facilities are found in the NISPOM, which is referenced by a clause in every classified contract. Any additional security requirements outside the scope of the NISPOM must be addressed in each contract that has such requirements.

The bottom line is, when a government agency negotiates a contract it must make sure to include all appropriate security requirements in the contract. Contractors are required to adhere to the requirements of their contracts. Failure to meet these obligations may have an adverse impact on a company's facility clearance and ability to continue doing business with the government.

Review Activity 3

Select True or False for this statement. When you are finished, see the Answer Key at the end of this Student Guide to check your answer.

		True	False
Contractors working on classified contracts are legally obligated to comply with the security provisions of the NISP.		○	○

Answer Key

Review Activity 1

The following are responsibilities of the FSO:

- Ensure compliance with the NISP
- Follow NISPOM guidelines
- Provide training for cleared individuals

Review Activity 2

If you are a government contractor working on a contractor-owned system at a contractor facility, you must follow the security provisions of **Chapter 8 of the NISPOM.**

Review Activity 3

		True	False
Contractors working on classified contracts are legally obligated to comply with the security provisions of the NISP.		●	○

Student Guide

Course: Introduction to Industrial Security

Lesson 3: Implementation of the NISP

Lesson Introduction

The National Industrial Security Program, also called the NISP, is a program to safeguard classified information entrusted to industry. The NISP is designed as a partnership between the U.S. Government and industry to protect classified information. Here's how the relationship works. When it is in the interest of the United States, cleared contractor facilities may be allowed to have access to classified information. The government sets requirements for the protection of this classified information, and industry implements these requirements with the government's advice, assistance, and oversight.

In this lesson, we are going to take a look at methods the government uses for implementing the industrial security program and various roles and responsibilities. By the end of this lesson you will be familiar with the term Cognizant Security Office (CSO), the Defense Security Service (DSS) role as CSO, and others in the role of CSO.

NISP Roles

1. CSAs and CSOs

Within the NISP there are four Cognizant Security Agencies, or CSAs. The CSAs are the:

- Central Intelligence Agency
- Department of Energy
- Nuclear Regulatory Commission
- Department of Defense.

The Department of Defense has agreements with 23 other Federal agencies to serve as CSA on their behalf. Each CSA has one or more Cognizant Security Offices, or CSOs, which administer the NISP. The CSO is the government organization that provides advice, assistance, and oversight. In most cases, the Defense Security Service serves as the CSO for the Department of Defense. In some instances other government offices assume some of the CSO functions. Keep this in mind. All of the entities mentioned above follow the same set of guidelines for classified contracts, outlined in the NISPOM.

2. Defense Security Service

The Department of Defense has delegated security oversight and administration to the Defense Security Service, or DSS, as the cognizant security office for most classified contracts within the Department of Defense. The CSO provides advice and assistance, and verifies contractor compliance with NISP requirements.

Although the Defense Security Service is usually the CSO within the Department of Defense, there are some exceptions to this. When contractors work on a military installation, the installation commander, who is ultimately responsible for security of the installation, may choose to retain some of the oversight functions of the CSO. In some cases when contractors work on a Special Access Program, the Program Manager retains some of the CSO responsibilities.

Security requirements that are outside the scope of the NISP require the oversight of the installation commander or of the agency or organization that levied the requirement upon the contract. In the case of a contractor performing entirely unclassified work on a military installation, DSS is not involved. Security oversight in this case would be primarily the responsibility of the installation commander.

3. Installation Commander or Facility Director

As a new security professional, you may have noticed that there are several individuals who are key personnel in the industrial security world. In this section, we are going to look at the role of an installation commander or facility director when contractors work on their installation or at their facility.

An installation commander has overall responsibility for the security of the installation. This includes such things as law enforcement, traffic regulation, physical security, information security, and information systems security. Contracts involving contractor employees working on a government installation or facility must include provisions for those employees to follow applicable security regulations.

When a contractor employee has access to a government-owned information system, the contract must provide for the employee to be subject to the security requirements of that system. When a contractor employee is a short-term or long-term visitor to a government facility or installation, he or she is subject to the security requirements of the host activity. When a contractor operates a cleared facility on a U.S. government installation, the installation commander may use the full range of services of DSS as the CSO, or may retain security cognizance over the facility's activities on the installation.

In later courses, you will learn more about this topic. For now, you should know that an installation commander or facility director has security responsibilities within the NISP, related to protecting classified information, as well as other security responsibilities which are outside the scope of the NISP.

Lesson Summary

As a security professional new to industrial security, you might not know all the details, but you must be familiar with certain aspects of the industrial security program. These are the things that you should be able to recall from this lesson.

There are four Cognizant Security Agencies in the National Industrial Security Program. They are the:

- Central Intelligence Agency
- Department of Energy

- Nuclear Regulatory Commission
- Department of Defense.

For classified contracts, the Department of Defense has delegated the security oversight and administration to the Defense Security Service, as the cognizant security office. An installation commander or Special Access Program Manager can retain security cognizance if they choose to.

Security requirements related to unclassified contracts, and most other requirements that are outside the scope of the NISP, are not overseen by the Defense Security Service. In most cases, security oversight for these requirements is the responsibility of the installation commander or the office that levied the requirement upon the contract.

As a security professional who is dealing with industrial security, it is important to know that you have resources that you can reach out to, should you have any security related questions. The cognizant security office can provide you with any guidance you need concerning industrial security requirements.

Review Activity 1

Fill in the blanks by placing each word in the correct sentence. Check your answers in the Answer Key at the end of this Student Guide.

A. Access
B. Retain
C. Delegated
D. Cognizant
E. Industry
F. Classified

1. There are four _____ Security Agencies that provide _____ with advice, assistance, and oversight with classified activities and contracts.

2. The Department of Defense has _____ the security oversight of its _____ contracts to the Defense Security Services.

3. A Special _____ Program (SAP) can _____ security cognizance if necessary.

Answer Key

Review Activity 1

A. Access
B. Retain
C. Delegated
D. Cognizant
E. Industry
F. Classified

1. There are four _____D_____ Security Agencies that provide _____E_____ with advice, assistance, and oversight with classified activities and contracts.

2. The Department of Defense has _____C_____ the security oversight of its _____F_____ contracts to the Defense Security Services.

3. A Special _____A_____ Program (SAP) can _____B_____ security cognizance if necessary.

Student Guide

Course: Introduction to Industrial Security

Lesson 4: Contract Administration

Lesson Introduction

Since Industrial Security involves both the government and industry working closely together, it is important that both parties understand and document all details prior to beginning the effort, such as security provisions and deliverable dates. Having written expectations in a contract allows everyone involved to follow the contract appropriately.

In this lesson, we are going to look at the contract process between the government and contractors, the responsibilities of the contracting officer's representative, and the contracting officer's technical representative, as well as what the statement of work is, and the function of the DD Forms 254 and 441.

Components of Contract Administration

1. Exploring the Contracting Process

Just like any acquisition for a product or service, the government has a process that it follows. This process is found in the Federal Acquisition Regulation, also known as the FAR, and the Defense Federal Acquisition Regulation Supplement, or DFARS.

Step 1
The Government has a need for a product or service.

Step 2
The Government Contracting Office prepares a Request for Proposal (RFP) for industry to view.

Step 3
Contractors that meet the qualifications of the RFP respond to the Government Contracting Office.

Step 4
The Government Contracting Office and the original requestor of the RFP choose the most qualified contractor to fulfill the need.

Step 5
The contract is awarded to the most qualified contractor. This contract will contain all of the Industrial Security provisions necessary for the task, and a copy of the NISPOM.

Step 6
Contractor conducts the work and adheres to all provisions of the contract and the NISP.

2. Contracting Officials

Contract administration involves several key individuals. In this lesson, we are going to take a look at the responsibilities of these government employees. They include the Contracting Officer, the Contracting Officer's Representative (COR), and the Contracting Officer's Technical Representative (COTR).

a. Contracting Officer

A Contracting Officer is a person with the authority to enter into, administer, and terminate contracts. The Contracting Officer typically has oversight and contract responsibility for numerous programs. Authority for administering contracts can be delegated to an Administrative Contracting Officer, or ACO. Authority for settling terminated contracts can be delegated to a Termination Contracting Officer, or TCO.

b. Contracting Officer's Representative (COR)

Another key individual is the Contracting Officer's Representative (COR) designated by the Contracting Officer. In a nutshell, a COR is assigned to a specific contract and is the person who oversees the process, making sure that all of the necessary requirements are being met for the Contracting Officer.

Some of the COR's responsibilities include determining whether a contractor has the need for access to classified information, verifying the contractor's facility clearance, as needed, sponsoring the contractor for a facility clearance, and communicating the security requirements for both the procurement process and contract performance. 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 Contracting Officer.

c. Contracting Officer's Technical Representative (COTR)

The Contracting Officer's Technical Representative (COTR) plays a very important role in Industrial Security. The COTR is not a contract expert; but rather, a subject matter expert, who could potentially have day-to-day contact with the contractor. An individual is chosen to be a COTR because he or she has the knowledge necessary to interact with the contractor concerning the service being provided to the government.

3. Statement of Work

Now we are going to briefly cover what a statement of work is and what is included in one. As a security professional in the industrial security field, you will hear this referred as an SOW. A statement of work is a document that is provided by the government to the contractor, which outlines, in detail, what will be required to complete a contract.

A few of the items covered in a SOW are:

- What the contract consists of
- Who will be working on the contract
- What clearance levels they will need
- How many hours they will be working
- Their hourly rates
- Any travel requirements.

The statement of work can be a useful document for security professionals and others to use in the preparation of the DD Form 254, Contract Security Classification Specification, which will be covered a little later.

4. DD Form 441: DoD Security Agreement

Now let's look at one of several forms used in the National Industrial Security Program. That form is the Department of Defense Security Agreement, or DD Form 441. This security agreement is a legally binding contract between the U.S. Government and the contractor. The security agreement is executed at the time a company receives a facility clearance, allowing the company to work on classified contracts.By signing the security agreement, the contractor makes a commitment to establish and maintain a security program that is in compliance with the requirements found in the National Industrial Security Program Operating Manual, or NISPOM.

The security agreement also establishes the government's authority to review the contractor's security program to ensure compliance. This document obligates the government to process personnel clearances for contractor employees as appropriate and to provide security classification guidance.

5. DD Form 254: DoD Contract Security Classification Specification

One very important form used in industrial security is the Department of Defense Contract Security Classification Specification, commonly referred to as the DD Form 254. The DD Form 254 is designed to provide a contractor with the security requirements and classification guidance needed to perform on a classified contract.

The DD Form 254 provides the contractor with specific clearance and access requirements, authorization to generate classified information and for classified storage at a contractor facility, classification guidance, guidance on how to handle public disclosure, and any other special security requirements above and beyond those required by the NISPOM.

To ensure that appropriate guidance is provided to the contractor, execution of the DD Form 254 should be a collaborative effort by a Contracting Officer or someone with contracting knowledge, for example the COR, a program manager or someone with program knowledge such as the COTR, and a security specialist who understands information and industrial security.

Lesson Summary

We have just covered a lot of information for someone new to industrial security. As your career progresses, you will learn much more about each of these topics. Let's review a few key things so you can walk away from this training with a basic understanding of the contract administration aspect of industrial security. When the government has a need for a service or product that industry can provide, it issues a request for proposal, and the process begins. Ultimately, the most qualified contractor is chosen and a contract is awarded. The contract includes clauses related to any security requirements that the contractor must follow.

- The **Contracting Officer** has the authority to enter into, administer, and terminate contracts, and make related determinations and findings.

- The **Contracting Officer's Representative (COR)** is designated by the Contracting Officer. A COR is assigned to a specific contract and is the person who oversees the process, making sure that all the necessary requirements are being met for the Contracting Officer.

- The **Contracting Officer's Technical Representative (COTR)** is a subject matter expert pertaining to the service or product the contractor provides. This person has regular contact with the contractor.

- A **statement of work** is a document that the government provides to the contractor, which outlines, in detail, what will be required to complete a contract.

- The **DD Form 441, DoD Security Agreement**, is a legally binding contract between the U.S. Government and the contractor. By signing the Security Agreement, the contractor makes a commitment to establish and maintain a security program that is in compliance with the requirements found in the NISPOM.

- The **DD Form 254, DoD Contract Security Classification Specification**, provides a contractor with specific security requirements and classification guidance needed to perform on a classified contract.

Review Activity 1

Match each word with the correct statement. Check your answers in the Answer Key at the end of this Student Guide.

A. DD Form 441	__	The program that covers protection of classified information by government contractors
B. SOW	__	A government employee with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings
C. Contracting Officer	__	This government employee is a subject matter expert who has regular contact with the contractor
D. NISP	__	The document that outlines in detail what will be required to complete a contract
E. DD Form 254	__	The document that establishes the government's authority to review the contractor's security program to ensure compliance
F. COTR	__	The form a contractor could use to determine if classified storage is authorized, and at what level

Answer Key

Review Activity 1

A. DD Form 441	D	The program that covers protection of classified information by government contractors
B. SOW	C	A government employee with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings
C. Contracting Officer	F	This government employee is a subject matter expert who has regular contact with the contractor
D. NISP	B	The document that outlines in detail what will be required to complete a contract
E. DD Form 254	A	The document that establishes the government's authority to review the contractor's security program to ensure compliance
F. COTR	E	The form a contractor could use to determine if classified storage is authorized, and at what level

Student Guide

Course: Introduction to Industrial Security

Lesson 5: Clearances

Lesson Introduction

Welcome to the lesson on clearances. Clearances are an important part of the Industrial Security Program. As a security professional, you will continue to learn much more about the many different clearances; however, for this lesson we are going to provide you with an overview of facility clearance, personnel clearance, eligibility, access, and visits, as they pertain to industrial security.

Contract Clearances

1. Facility Clearance

A facility clearance is an administrative determination that a company is eligible for access to classified information at a certain classification level and at all lower classifications. Although this is called a facility clearance, it is not the building or structure that is cleared. Instead, it is actually the individuals who run, own, and manage that facility that are cleared. A facility clearance is not granted until personnel clearances for key management personnel of the facility are granted.

In order for employees of a contractor, or its facility, to have access to classified information, the contractor or facility must first have the facility clearance granted. Likewise, in order for a contractor or facility to be in possession of classified material, the facility clearance must be granted and safeguarding capabilities approved. There are five essential elements to obtaining a facility clearance:

- Sponsorship
- Security agreement
- A certificate pertaining to foreign interests
- Organization
- Key management personnel clearances.

2. Personnel Clearance

People make an organization run and meet its mission. When a facility security clearance is granted, it is not the actual building; but rather, the individuals who are working within the organization that are cleared. Let's take a brief look at personnel clearances and how they play an important part in industrial security.

In essence, a facility security clearance is granted to allow the clearing of employees who have a need to handle classified information, either in the facility itself, at another cleared facility, or at a government installation. The type of work that will be performed by the facility determines what level clearance the personnel need.

Here's how the personnel clearance process works:

a. First, the employer determines that the employee needs access to classified information to do his or her job and verifies that the employee is a U.S. citizen. If these conditions exist, the person may apply, through their employer's security office, for a clearance.

b. At that point the applicant completes a Questionnaire for National Security Positions, also known as Standard Form 86 or SF-86. This form is normally completed electronically using software provided by the investigative agency.

c. Then, the SF-86 is transmitted to the Defense Industrial Security Clearance Office, also known as DISCO. Security specialists at DISCO determine whether the request for a clearance is legitimate, and if so, what type of investigation is needed prior to making a decision on the application.

d. If the decision is made to move ahead with the investigation, then a preliminary check is conducted and a full investigation is scheduled, which may include record checks and personal interviews.

e. The information collected throughout the investigation is recorded in a report that is read by an adjudicator, who makes a decision to grant, or not to grant, the clearance.

f. Finally, the individual and their organization are notified of the decision.

As a security professional, you will learn about this process in more depth. For now, it is important for you to understand that personnel clearances involve a potentially lengthy process, but are imperative for a cleared facility to meet their industrial security responsibilities.

3. Eligibility

Now let's look at eligibility as it pertains to personnel clearances within industrial security. Contractor employees may be granted personnel clearances only up to the level of the facility clearance of their employer. Individual employees of the facility who need access to classified information to perform their duties must each apply for a personnel security clearance. The applications are submitted through the facility's security office to the Defense Industrial Security Clearance Office, also known as DISCO.

An eligibility determination is made by the central adjudication facility (CAF) based on national standards as stated in the DoD Personnel Security Regulation, DoD 5200.2-R. More details about this process are included in the Introduction to Personnel Security web-based training course.

When an eligibility determination is made, DISCO enters the eligibility into the Joint Personnel Adjudication System, or JPAS. JPAS is the Department of Defense's official system of record for contractor eligibility and access. The security office of the employing facility will then be able to grant access up to the level for which the individual is eligible, based on his or her need for access. This access is also recorded in JPAS. Eligibility

plus access as recorded in JPAS are considered to be an individual's personnel security clearance.

4. Access

Once an individual has been granted eligibility, they will be granted access by the Facility Security Officer, or a designee. Access is the level of classified information that may be disclosed to an individual. An individual's access can never be higher than the level of the facility clearance or the level of eligibility granted by the CAF.

The government requires continued evaluation of the need for personnel clearances. So, it is not unlikely that an individual could change access levels at different times during his or her career based on assigned duties. When access is no longer needed, the Facility Security Officer must terminate the employee's access.

Basically, what you should be familiar with at this point is that one's eligibility level, which is determined by a central adjudication facility, plus designated access, which is determined by the facility's security office, equals the individual's personnel security clearance.

5. Visits

There will undoubtedly be times when industry and government workers have to work at each other's facilities while fulfilling a contract. When a visitor must have access to classified information, it is the responsibility of the party who is going to disclose the information to ensure that the visitor is an authorized person. To be an authorized person one must have a personnel clearance at the appropriate level and must have a need to know the information. Visit procedures found in Chapter 6 of the National Industrial Security Program Operating Manual or NISPOM provide for this.

Verification of a visitor's clearance, also referred to as eligibility and access, is normally done through JPAS. For organizations that do not use JPAS, the FSO may send a visit authorization letter with this information. Need-to-know is determined based upon the person's professional duties. This may be related to a contract between the sending and receiving facilities, or some other factor that clearly establishes a legitimate reason for the person to have access to the information.

Lesson Summary

As a security professional, you will learn much more about these topics in the future. For now, what is important is that you can recall these concepts:

- An actual building is not what receives a facility clearance; but rather, the organization, including the key management personnel who run the facility.
- Facility clearance is granted based on five elements:
    - Sponsorship

  - Security Agreement (DD form 441)
  - Certificate Pertaining to Foreign Interest (SF-328)
  - Business Structure
  - Organizational Clearance of Key Management Personnel (KMP)

- Personnel clearances are required prior to an individual having access to classified information.
- Eligibility plus access recorded in JPAS is synonymous with a personnel clearance.
- Access may be granted after a favorable eligibility determination.
- An individual's access level cannot be higher than the level of the facility clearance of his or her employer.
- Visits to and from classified facilities require preparations that include validating clearance levels and need-to-know.

Review Activity 1

Fill in the blanks by matching each word to the sentence in which it belongs. Check your answers in the Answer Key at the end of this Student Guide.

A. Eligibility	__	A cleared individual can only have access at the _____ level as the facility clearance.
B. JPAS	__	For the purpose of a visit to another cleared facility, a clearance can be verified by looking in _____.
C. Same	__	The issuance of _____ is the responsibility of the Central Adjudication Facility (CAF).

Answer Key

Review Activity 1

A. Eligibility	C	A cleared individual can only have access at the _____ level as the facility clearance.
B. JPAS	B	For the purpose of a visit to another cleared facility, a clearance can be verified by looking in _____.
C. Same	A	The issuance of _____ is the responsibility of the Central Adjudication Facility (CAF).