

Student Guide

# Clearances in Industrial Security: Putting It All Together

---

## *Lesson 1: Course Introduction*

### **Contents**

Introduction .....	2
Welcome .....	2
Roles .....	2
Course Objectives .....	2

## Introduction

### **Welcome**

"I'm Ellen Johnson. I started my own company, Johnson Technology Services, five years ago. It hasn't been easy, but I've been able to slowly grow my business. The federal government is my biggest client. We recently won a classified contract—our first ever! This is a big step for my company that may lead to future opportunities.

I know that we need to go through some kind of process before we can access the information we need to fulfill our contract, but I'm not 100 percent clear on that."

Even though Johnson Technology Services was awarded the contract, Ellen is correct that this does not mean they are cleared to access classified information.

But what clearances do they need? And who needs to be cleared? How do they obtain those clearances? How might foreign ownership, control, or influence (FOCI) impact those clearances? And who will be involved in processing those clearances?

Welcome to the Clearances in Industrial Security: Putting It All Together course.

### **Roles**

Determinations for eligibility for access to classified information are carefully evaluated to ensure they are consistent with national security. Determinations are made for companies as well as individuals, and these clearances work together to ensure the protection of national security information. Many government personnel and entities play a role in ensuring that eligibility is granted only to those companies and individuals who will adequately protect the information. In this course, you will learn how these roles work together to make clearance determinations.

### **Course Objectives**

Here are the course objectives:

- Identify the purpose of facility and personnel security clearances
- Identify what is required for an individual to obtain a personnel security clearance
- Identify the elements for obtaining a facility clearance
- Identify how facility and personnel security clearances are related
- Identify the effect of foreign ownership, control, or influence on a facility's clearance

## Student Guide

# Clearances in Industrial Security: Putting It All Together

---

## *Lesson 2: FCL and PCL Overview*

### Contents

Introduction .....	2
Objectives.....	2
Definitions, Purpose, and Levels .....	2
FCL and PCL Comparisons .....	2
Scenario .....	3
Review Activities .....	4
Review Activity 1 .....	4
Conclusion .....	5
Lesson Summary.....	5
Answer Key .....	6
Review Activity 1 .....	6

## Introduction

### **Objectives**

The National Industrial Security Program (NISP) is designed to safeguard classified information entrusted to private industry. But which companies and personnel can be trusted with classified information?

In this lesson, you will learn about the purpose of facility and personnel security clearances and the levels at which they are granted.

Here are the lesson objectives.

- Identify the purpose of facility and personnel security clearances
- Identify the levels at which facility security clearances are granted
- Identify the levels at which personnel security clearances are granted

## Definitions, Purpose, and Levels

### **FCL and PCL Comparisons**

Facility security clearances (FCLs) and personnel security clearances (PCLs) are closely tied to each other. They serve a similar purpose and are granted at comparable classification levels based on access requirements of a classified contract. Note that PCLs must be tied to an FCL. In order to be cleared, an individual must be associated with a cleared company and there must be a need for access to classified information.

### **Definition and Purpose**

An FCL is an administrative determination that, from a security viewpoint, a *company* is eligible for access to classified information of a certain category and all lower categories. As you will learn, a company's eligibility for an FCL is impacted by the presence of foreign ownership, control, or influence (FOCI) and whether it can be mitigated.

#### **FOCI**

A U.S. company is considered to be operating under foreign ownership, control, or influence whenever a foreign interest has the power—direct or indirect, whether or not exercised, and whether or not exercisable—to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

A PCL is an administrative determination that, from a security viewpoint, an *individual* is eligible for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Both FCLs and PCLs are determinations for eligibility to classified information. The difference between the two is the type of entity for which eligibility is established. FCLs are granted to companies, meaning that the people who own, run, and manage the company have been cleared, in addition meeting other administrative requirements. PCLs are granted to individuals, such as employees who have a need to access classified information or key management personnel in connection with the FCL.

### **Levels**

FCLs and PCLs are granted at the Confidential, Secret, and Top Secret classification levels. A company or an individual can only access information at or below the level of clearance granted. When sponsored by a facility, an employee's PCL is capped at the level of the FCL. Some employees may have higher clearances due to an affiliation with the National Guard or Reserves, but their access is capped at the level of the FCL for their contractor work.

In some cases, companies will require additional accesses and eligibility criteria. For example, when a classified contract requires access to a Special Access Program (SAP) or Sensitive Compartmented Information (SCI) additional investigative requirements are needed. When working with SCI or a SAP, individuals must meet access eligibility criteria in addition to a PCL in order to access these types of information.

### **Scenario**

Remember Ellen Johnson? Her company, Johnson Technology Solutions, has just been awarded a Secret contract—their first classified contract. Take a moment to consider what needs to happen before Johnson Technology Solutions can access the information it needs to fulfill its contract with the government.

First, Johnson Technology Solutions will need an FCL. Key management personnel, or KMP, and employees who will support the contract will need PCLs. Since information can only be accessed at or below the level of eligibility granted, the FCL and any PCLs sought in support of the contract will need to be at the Secret level.

## Review Activities

### **Review Activity 1**

*Question 1 of 3.* Which of the following is an administrative determination that a company is eligible for access to classified information?

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

- Facility security clearance (FCL)
- Personnel security clearance (PCL)
- Both FCL and PCL

*Question 2 of 3.* Which of the following is an administrative determination that a contractor employee is eligible for access to classified information?

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

- Facility security clearance (FCL)
- Personnel security clearance (PCL)
- Both FCL and PCL

*Question 3 of 3.* Which of the following may be granted at the Confidential, Secret, or Top Secret level?

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

- Facility security clearance (FCL)
- Personnel security clearance (PCL)
- Both FCL and PCL

## **Conclusion**

### ***Lesson Summary***

You have completed the FCL and PCL Overview lesson.

## Answer Key

### **Review Activity 1**

*Question 1 of 3.* Which of the following is an administrative determination that a company is eligible for access to classified information?

- Facility security clearance (FCL) (correct response)
- Personnel security clearance (PCL)
- Both FCL and PCL

**Feedback:** *An FCL is a determination that a company can be entrusted with classified information.*

*Question 2 of 3.* Which of the following is an administrative determination that a contractor employee is eligible for access to classified information?

- Facility security clearance (FCL)
- Personnel security clearance (PCL) (correct response)
- Both FCL and PCL

**Feedback:** *A PCL is a determination that a person is able and willing to safeguard classified information.*

*Question 3 of 3.* Which of the following may be granted at the Confidential, Secret, or Top Secret level?

- Facility security clearance (FCL)
- Personnel security clearance (PCL)
- Both FCL and PCL (correct response)

**Feedback:** *Both FCLs and PCLs are granted at the Confidential, Secret, and Top Secret levels. Additional safeguards may be required for some classified information.*



## Student Guide

# Clearances in Industrial Security: Putting It All Together

---

## *Lesson 3: FCL and PCL Processes and Relationships*

### Contents

Introduction .....	3
Objectives.....	3
Steps for Obtaining an FCL.....	3
Overview .....	3
Sponsorship.....	4
FCL Orientation Handbook .....	4
CAGE Code.....	4
Information Gathering .....	4
PCLs for KMP .....	6
Eligibility Determination .....	7
FCL Summary .....	7
Steps for Obtaining a PCL.....	8
Overview .....	8
Identification of Need-to-Know .....	8
Information Gathering .....	9
Package Reviews .....	9
Investigation .....	9
Adjudication.....	9
Eligibility Determination .....	12
PCL Summary .....	12
FCL/PCL Relationship.....	12

---

Relationships .....	12
Review Activities .....	14
Review Activity 1 .....	14
Review Activity 2 .....	15
Review Activity 3 .....	16
Conclusion .....	17
Lesson Summary.....	17
Answer Key .....	18
Review Activity 1 .....	18
Review Activity 2 .....	19
Review Activity 3 .....	20

## Introduction

### Objectives

Before Johnson Technology Services can access the classified information necessary to fulfill its contract, it will need to get a facility security clearance (FCL) and its key management personnel and staff will need to obtain personnel security clearances (PCLs). In this lesson, you will learn the process for obtaining an FCL, the process for obtaining a PCL, and the relationship between FCLs and PCLs.

Here are the lesson objectives.

- Identify what is required for an individual to obtain a PCL
- Identify the factors used to determine an individual's eligibility for a PCL
- Identify the elements for obtaining an FCL
- Identify the factors used to determine a company's eligibility for an FCL
- Identify how FCLs and PCLs are related
- Identify when a company can sponsor an employee for a PCL
- Identify when an FCL is dependent on PCLs
- Identify the level of classified information that can be handled based on the FCL and PCL granted

## Steps for Obtaining an FCL

### Overview

Obtaining an FCL is a multi-step process.

- *Sponsorship*: First, a company must be sponsored for an FCL based upon a need to access classified information.
- *FCL Orientation Handbook*: Once the Defense Security Service Facility Clearance Branch (DSS FCB) receives and accepts the FCL request, it will send the FCL Orientation Handbook to the company's Facility Security Officer (FSO).
- *CAGE Code*: If the company does not already have a Commercial and Government Entity (CAGE) Code, one must be obtained prior to FCL issuance.
- *Information Gathering*: The company must provide certain information about itself in the Electronic Facility Clearance System (e-FCL).
- *PCLs for KMP*: Specific Key Management Personnel (KMP) must obtain PCLs.
- *Eligibility Determination*: Finally, the Department of Defense Central Adjudication Facility (DoD CAF) makes an eligibility determination.

Let's take a look at each step of the process in more detail.

## ***Sponsorship***

A contractor or prospective contractor cannot apply for its own FCL. To obtain an FCL, the contractor must be sponsored by either a company cleared to participate in the National Industrial Security Program (NISP) or a Government Contracting Activity (GCA) when a definite classified procurement need has been established. The DSS FCB has a sample sponsorship letter that the sponsoring organization may use to submit the sponsorship to FCB. The sample sponsorship letter is available on the Course Resources page.

## ***FCL Orientation Handbook***

The FCL Orientation Handbook provides guidance to the FSO on the FCL process, including business structure and excluded tier entities, the e-FCL process, accounts and systems, preparing for the FCL Orientation meeting, and where to find FSO training. The FCL Orientation Handbook is available on the Course Resources page.

## ***CAGE Code***

DSS uses a CAGE Code to track basic facility information. The sponsored company must obtain a CAGE Code if it does not already have one before an FCL can be issued. To obtain a CAGE Code, a company can register online with the System for Award Management (SAM) database.

## ***Information Gathering***

The company's prospective FSO will use the FCL Orientation Handbook and work with the DSS FCB to determine which forms must be uploaded to e-FCL. While this varies based on management structure, all companies must submit:

- The SF 328, the Certificate Pertaining to Foreign Interest
- A summary data sheet containing basic information about the company such as the company's website, stock information, and previous names
- Corporate governance documents
- Organizational chart
- A list of KMP
- A tiered parent list, if applicable
- The DD Form 441, the Department of Defense Security Agreement
- The DD Form 441-1, the Appendage to the Department of Defense Security Agreement, which lists (if applicable) cleared divisions or branches included in and covered by the provisions of the organization's Security Agreement and Certificate Pertaining to Foreign Interest

The SF 328, DD Form 441, and DD Form 441-1 are all available on the Course Resources page.

*NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.*

### **Forms Required**

#### *SF 328, Certificate Pertaining to Foreign Interests*

- Certificate pertaining to a company's foreign interests
- Execute two original SF 328 forms for DSS and contractor retention
- SF 328 must be signed by an employee or representative of the company who has actual authority to execute agreements with the U.S. Government on behalf of the company
- Upload signed SF 328 into e-FCL
- Provide all supplemental responses to affirmative SF 328 questions

#### *Summary Data Sheet*

- List company website
- Include stock information
- List all previous business names
- List all Tiered Parents
- Match number of Directors in Articles of Organization to Company Bylaws
- List all addresses dating back 10 years
- Current Chairman of the Board

#### *KMP Form*

- Spell out entire KMP names
- Social Security Number not required for excluded KMP
- Citizenship of all personnel listed as required to be cleared
- KMP must match the Articles of Organization, bylaws or amendments

#### *Tiered Parent List (if applicable)*

- List of all Parent Companies

#### *DD Form 441*

- Agreement between the organization and the U.S. Government that details the security responsibilities of both the cleared organization and the U.S. Government
- Execute two original DD 441 forms for DSS and contractor retention
- DD 441 must be signed by an employee or representative of the company who has actual authority to execute agreements with the U.S. Government on behalf of the company
- Upload signed DD 441 into e-FCL upon receipt of countersignatures from DSS

#### *DD Form 441-1 (if applicable)*

- Attachment to the DD Form 441 listing cleared divisions or branch offices that are included in and covered by the provisions of the organization's Security Agreement and Certificate Pertaining to Foreign Interest

## ***PCLs for KMP***

Before a company can be cleared, specified KMP must first be cleared. Which KMP are required to be cleared is based on the management structure and organization of the facility. The DSS Industrial Security Representative (IS Rep) can help identify those KMP who must be cleared. Other KMP may be excluded unless they will require access to classified information. The DSS FCB will initiate the PCL process for KMP who must be cleared.

*NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.*

### **KMP Requiring PCLs**

#### *Sole Proprietorship*

- Owner
- Senior Management Official (SMO), if other than owner
- Facility Security Officer (FSO), if other than owner

#### *General Partnership*

- SMO
- FSO
- All general partners

Exceptions: If full management control resides in a managing partner, then that partner must be cleared. If full management control resides in an executive committee, then all committee members must be cleared.

#### *Limited Partnership*

- SMO
- FSO
- All general partners

Exceptions: If full management control resides in a managing partner, then that partner must be cleared. If full management control resides in an executive committee, then all committee members must be cleared. Limited partners need PCLs only if they impact classified contract performance or need access to classified information.

#### *Limited Liability Company (LLC)*

- SMO
- FSO
- All LLC members must be cleared or excluded.
  - Eligibility for classified access depends on the member's duties, ownership share, and management influence.
  - Managers with delegated decision-making authority and the ability to bind the LLC must be cleared or excluded.
  - Non-member officials who can enter into contracts must be cleared or excluded.

*College/University*

- SMO
- FSO
- Chief Executive Officer (CEO)
- Other officers/officials with accountability for classified contracts
- All regents/trustees/directors

Exceptions: Exclude regents/trustees/directors who do not require access and cannot affect contract performance. Leave a legal quorum of executives who are eligible. Exclude regents/trustees/directors if they have delegated management control to an executive committee. All committee members must be cleared.

*Note:* Other officials, as determined by the Cognizant Security Agency (CSA), must be granted PCLs or be excluded from classified access pursuant to NISPOM paragraph 2-106. (Reference source: NISPOM paragraph 2-104)

***Eligibility Determination***

To be granted an FCL, the company must meet four main eligibility requirements:

- First, the company must require access to the classified information in connection with a legitimate U.S. government or foreign government requirement.
- Next, the company must be located in the U.S. or its territories and be organized and existing under the laws of any of the 50 states, the District of Columbia, Puerto Rico, or a formally acknowledged American Indian or Alaska Native tribe.
- Also, the company must have a reputation for integrity and lawful conduct in its business dealings. The company and its KMP must not be barred from participating in U.S. government contracts.
- Finally, the company must not be under foreign ownership, control, or influence (FOCI) to such a degree that the granting of the FCL would be inconsistent with national security interests.

The DSS FCB may issue an interim FCL with IS Rep concurrence if these requirements have been met and KMP have been issued interim PCLs. Even after an FCL is granted, the company must continue to meet these eligibility requirements and report any change in conditions that may impact it.

***FCL Summary***

Now that you've seen the process for obtaining an FCL, think for a moment about what Ellen needs to do. As a refresher, Ellen owns Johnson Technology Services, which has just been awarded its first classified contract and will need access to classified information.

First, the sponsoring GCA or cleared contractor must submit the sponsorship letter and proof of contractual need to DSS. The FSO must review the FCL Orientation Handbook. Johnson Technology Services must obtain a CAGE Code if one has not already been issued and gather the necessary information about the company to upload to e-FCL. Ellen must work with her company's IS Rep to determine which KMP will need PCLs before an FCL can be granted.

If you would like to learn more about FCLs, see the Facility Clearances in the NISP course available through the Security, Training, Education, and Professionalization Portal (STEPP).

## Steps for Obtaining a PCL

### Overview

Obtaining a PCL is a multi-step process.

- *Identification of Need-to-Know:* The process begins when a cleared company identifies an employee who will require access to classified information in performance of a classified contract. When the company is in the process of obtaining an FCL, the DSS FCB initiates the PCL process for KMP.
- *Information Gathering:* The employee must provide information about him- or herself.
- *Package Reviews:* The security clearance application must be reviewed for completeness and accuracy by the FSO.
- *Investigation:* A background investigation is conducted on the employee.
- *Adjudication:* The results of the investigation are reviewed and compared with qualifying criteria.
- *Eligibility Determination:* An eligibility determination is made.

### Identification of Need-to-Know

Once a cleared company determines an employee will require access to classified information in performance of tasks or services related to the fulfillment of a classified contract, the company initiates the PCL process. Individuals cannot apply for PCLs without association with a cleared company and a need for access. The company must make an effort to keep the number of PCLs to an absolute minimum based on the contractual need to access classified information.

The company's FSO initiates the process by submitting a clearance request using the Joint Personnel Adjudication System (JPAS). If the applicant already has an active JPAS record, an investigation may not be required. The company will need to assume ownership of the applicant's JPAS record before proceeding. If the applicant requires an upgrade to the level of a current PCL, has never held a PCL, or previous



access was terminated more than 24 months ago, this is referred to as an initial clearance.

### ***Information Gathering***

There are three things the employee must submit electronically for an initial clearance request:

- The electronic questionnaires for investigations processing (e-QIP)
- Signature forms
- Fingerprints via Secure Web Fingerprint Transmission (SWFT)

Collectively, these are referred to as the security clearance package.

### ***Package Reviews***

After the employee completes the security clearance package, the FSO informs the applicant, either in writing or verbally, that the package will be reviewed for adequacy and completeness only, and then reviews it before submitting it to the Personnel Security Management Office for Industry (PSMO-I). The PSMO-I checks the package for completeness, then forwards it to the Investigative Service Provider (ISP). For DoD, the ISP is the Office of Personnel Management (OPM). While reviewing the security clearance package, the PSMO-I will make an interim PCL determination. If there is no evidence of adverse information, PSMO-I will grant an interim PCL and update JPAS accordingly. In some cases, applicants may be allowed to work with an interim clearance, provided the company has at least an interim FCL.

### ***Investigation***

OPM also reviews the security clearance package prior to opening the investigation. If the package is incomplete, OPM will coordinate with the FSO (or FCB, in the case of a company in-process for an FCL) to resolve any issues. Once OPM completes the investigation, the results are submitted to the DoD CAF.

### ***Adjudication***

The DoD CAF reviews the results of the investigation and compares them with the established qualifying criteria for eligibility for access to classified information in order to make a final eligibility determination.

You may also learn more about each of the adjudicative guidelines through the Personnel Security Shorts available through the Center for Development of Security Excellence's website.

*NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.*

### **13 Adjudicative Guidelines**

#### *Allegiance to the United States*

An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States. Example: membership in an organization that supports the overthrowing of the U.S. government

#### *Foreign Influence*

A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure. Example: foreign financial interest or employment that may affect the individual's security responsibility

#### *Foreign Preference*

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

#### *Sexual Behavior*

Sexual behavior is a security concern if it involves a criminal offense; indicates a personality or emotional disorder; may subject the individual to coercion, exploitation, or duress; or reflects lack of judgment or discretion. Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance. Example: arrest for a sexual-related crime

#### *Personal Conduct*

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Example: subject left previous employment due to fraud

#### *Financial Considerations*

An individual who is financially overextended is a risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts. Example: a history of not meeting financial obligations or an inability or unwillingness to satisfy debts

#### *Alcohol Consumption*

Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, and failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness. Example: treatment for alcohol abuse

#### *Drug Involvement*

Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information. Example: recent drug use, illegal drug possession, or drug dependence

#### *Psychological Conditions*

Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social, and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. Example: information that suggests that an individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability

#### *Criminal Conduct*

A history or pattern of criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. Example: felony arrests, multiple misdemeanor arrests, or imprisonment for over one year

#### *Handling Protected Information*

Noncompliance with security regulations raises doubts about an individual's trustworthiness, willingness, and ability to safeguard classified information. Example: multiple security violations

#### *Outside Activities*

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

#### *Use of Information Technology Systems*

Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information. Example: viewing unauthorized websites

## ***Eligibility Determination***

Each case is judged on its own merits. The DoD CAF makes an eligibility determination, and access is granted by the contractor. Any doubt regarding whether access to classified information is clearly consistent with national security must be resolved in favor of national security. While the majority of applicants are granted eligibility, complicating factors may delay a decision or result in a denial or revocation of previously granted security eligibility. For industry, if the applicant's request is not clearly consistent with national security interests, the DoD CAF forwards the case to the Defense Office of Hearings and Appeals (DOHA) to determine whether it is clearly consistent with the national interest to grant or continue security eligibility for the applicant.

## ***PCL Summary***

Now that you've seen the process for obtaining a PCL, think for a moment what an employee of Johnson Technology Services needs to do to obtain a PCL.

Once the FSO at Johnson Technology Services has verified that the employee requires access to classified information, the FSO must determine if the employee is already cleared and, if not, submit a clearance request using JPAS. If the employee has not held a clearance at the appropriate level in the past 24 months, the employee must complete the e-QIP and signature forms and submit fingerprints via SWFT. The clearance package is routed from the FSO to the PSMO-I to the ISP, which is OPM for DoD. All three review the package for completeness. The PSMO-I also determines eligibility for an interim clearance. OPM conducts the investigation and provides the results to the DoD CAF, who reviews the results of the investigation and compares them with the 13 adjudicative guidelines to determine eligibility for access to classified information. The DoD CAF or, if applicable, DOHA, judges the case on its own merits to decide whether access to classified information is consistent with national security and makes an eligibility determination.

If you would like to learn more about PCLs, see the Personnel Clearances in the NISP course available through STEPP.

## **FCL/PCL Relationship**

### ***Relationships***

FCLs and PCLs are connected in two ways. Eligibility for an FCL is dependent on essential KMP successfully obtaining PCLs. FCLs and PCLs also impact the level of classified material that can be handled.

### **Dependency**

The PCLs for KMP are required in connection with the request for an FCL. For example, at Johnson Technology Services, the company's eligibility for an FCL depends on whether the owner, Ellen Johnson, can obtain a PCL. If an interim PCL for an individual required to be cleared in connection with the FCL is withdrawn, the individual must be removed from access or the interim FCL will also be withdrawn.

### **Classification Level**

Keep in mind that a facility can only access classified information at the highest level granted by its FCL, and an individual can only access information at the highest level granted by his or her PCL. These can impact each other if the FCL and an employee's PCL are at different levels.

For example, if an employee has a Top Secret PCL and works in a facility with a Secret FCL, the employee can only access information at a Secret classification level or below.

Another example is an employee with a Secret PCL who works in a facility with a Top Secret FCL. Even though the facility can access Top Secret information, the employee can still only access information at a Secret classification level or below.

## Review Activities

### **Review Activity 1**

*For each statement, select whether it is true or false. Check your answer in the Answer Key at the end of this Student Guide.*

A contractor can apply for its own FCL.

- True
- False

A CAGE Code is required for a company to be issued an FCL.

- True
- False

A foreign company may be eligible for an FCL.

- True
- False

## **Review Activity 2**

*Indicate who performs each task in the PCL process below. Check your answer in the Answer Key at the end of this Student Guide.*

Determines eligibility for an interim clearance

- FSO
- PSMO-I
- OPM
- CAF

Makes the final eligibility determination

- FSO
- PSMO-I
- OPM
- CAF

Conducts the investigation

- FSO
- PSMO-I
- OPM
- CAF

Initiates the clearance process

- FSO
- PSMO-I
- OPM
- CAF

### **Review Activity 3**

When is FCL eligibility dependent on a PCL?

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

- Any time a PCL request is submitted with an FCL request
- When the PCL is for a KMP who is not excluded
- When the FCL sponsor requires PCLs for staff
- Never



## **Conclusion**

### ***Lesson Summary***

You have completed the FCL and PCL Processes and Relationships lesson.

## Answer Key

### **Review Activity 1**

A contractor can apply for its own FCL.

- True
- False (correct response)

**Feedback:** A contractor must be sponsored for an FCL by another cleared company or the GCA.

A CAGE Code is required for a company to be issued an FCL.

- True (correct response)
- False

**Feedback:** The CAGE Code is used by DSS to track basic facility information.

A foreign company may be eligible for an FCL.

- True
- False (correct response)

**Feedback:** To be eligible for an FCL, the company must be organized and existing under the laws of any of the 50 states, the District of Columbia, or Puerto Rico.

## **Review Activity 2**

Question 1 of 4. Determines eligibility for an interim clearance

- FSO
- PSMO-I (correct response)
- OPM
- CAF

**Feedback:** *The PSMO-I determines if an individual is eligible for an interim clearance while checking the security clearance package for completeness.*

Question 2 of 4. Makes the final eligibility determination

- FSO
- PSMO-I
- OPM
- CAF (correct response)

**Feedback:** *The DoD CAF (or DOHA, if applicable) reviews the results of the investigation and makes a final eligibility determination by comparing the results with the 13 adjudicative guidelines.*

Question 3 of 4. Conducts the investigation

- FSO
- PSMO-I
- OPM (correct response)
- CAF

**Feedback:** *OPM conducts the investigation after reviewing the security clearance package for completeness.*

Question 4 of 4. Initiates the clearance process

- FSO (correct response)
- PSMO-I
- OPM
- CAF

**Feedback:** *The company's FSO initiates the process by submitting a clearance request using JPAS.*

### **Review Activity 3**

When is FCL eligibility dependent on a PCL?

- Any time a PCL request is submitted with an FCL request
- When the PCL is for a KMP who is not excluded (correct response)
- When the FCL sponsor requires PCLs for staff
- Never

**Feedback:** *FCL eligibility depends on KMP successfully obtaining PCLs.*

## Student Guide

# Clearances in Industrial Security: Putting It All Together

---

## *Lesson 4: FOCI and the FCL*

### Contents

Introduction .....	2
Objectives.....	2
Definition .....	2
What Is FOCI?.....	2
FOCI Determination .....	2
Overview .....	2
FOCI Factors.....	2
Impact of FOCI on the FCL.....	3
FCL Eligibility .....	3
Eligibility Reassessment .....	3
Scenario .....	3
Review Activities .....	5
Review Activity 1 .....	5
Review Activity 2 .....	5
Conclusion .....	6
Lesson Summary.....	6
Answer Key.....	7
Review Activity 1 .....	7
Review Activity 2 .....	7

## Introduction

### **Objectives**

Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. government to allow foreign investment consistent with the national security interests of the United States. However, when a U.S. company seeks or holds a facility clearance (FCL) it is important to assess whether foreign ownership, control, or influence (FOCI) indicators are present, as well as the source, nature, and extent of those indicators, to ensure the protection of classified national security information.

Here are the lesson objectives.

- Define FOCI
- Identify the effect of FOCI on an FCL

## Definition

### **What Is FOCI?**

A U.S. company is considered to be operating under FOCI whenever a foreign interest has the power—direct or indirect, whether or not exercised, and whether or not exercisable—to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

## FOCI Determination

### **Overview**

When evaluating a company's initial and continued eligibility for an FCL, the Defense Security Service (DSS) makes FOCI determinations on a case-by-case basis. DSS uses the information provided on the SF 328, Certificate Pertaining to Foreign Interest, and any other relevant information to determine whether a company is under FOCI to such a degree that granting or allowing a company to continue to hold an FCL would be inconsistent with national security interests.

### **FOCI Factors**

When making a FOCI determination, DSS considers several factors:

- Record of economic and government espionage
- Record of engagement in unauthorized technology transfer
- Record of compliance with U.S. laws, regulations, and contracts
- Type and sensitivity of the information that will be accessed
- Source, nature, and extent of FOCI

- Majority or substantial minority position in the company
- Immediate, intermediate, and ultimate parent companies
- Prior relationships between the U.S. company and the foreign interest
- Nature of any bilateral and multilateral security and information exchange agreements
  - Political and military relationship between the countries
- Ownership and control by a foreign government
- Any other factors that indicate or demonstrate foreign influence

### ***Impact of FOCI on the FCL***

A U.S. company determined to be under FOCI is ineligible for an FCL unless and until security measures have been put into place to mitigate FOCI.

To learn more about the FOCI determination process and FOCI mitigation plans, see the *Understanding FOCI* course available through the Security, Training, Education, and Professionalization Portal (STEPP) and the *FOCI Short* available on the Center for Development of Security Excellence's website.

## **FCL Eligibility**

### ***Eligibility Reassessment***

Once granted, DSS reassesses the company's eligibility to maintain the FCL on a continuing basis. A change in conditions, such as a change in ownership, control, or influence; indebtedness; or a foreign intelligence threat, may justify adjustments to the security terms under which a contractor is cleared or, alternatively, require the use of a FOCI mitigation or negation agreement.

Depending on circumstances, DSS may determine that a contractor is no longer under FOCI or, conversely, that a contractor is no longer eligible for an FCL. If a contractor does not have a current or pending requirement for access to classified information, DSS will administratively terminate the FCL.

### ***Scenario***

Ellen: "Business has been going well, so I've decided to merge with another small business—that just happens to have a foreign investor—so we can pursue larger contracts."

Will the other company's foreign investor impact Johnson Technology Services' FCL?

Yes, it may impact the company's FCL.

Due to the change in ownership, DSS will need to reassess the company's eligibility for an FCL, including a determination as to whether the new company is under FOCI to such a degree that granting an FCL would be inconsistent with U.S. national security interests. DSS may determine that Johnson Technology Services is still eligible for an FCL, that a FOCI mitigation plan must be put into place, or that the company is no longer eligible for an FCL.



## Review Activities

### Review Activity 1

A U.S. company is considered to be operating under FOCI when a foreign interest has \_\_\_\_\_ to make decisions that may compromise classified information.

*Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.*

- Direct power
- Indirect power
- Exercised power
- Unexercised power

### Review Activity 2

*For each statement below, select whether it is true or false. Then check your answers in the Answer Key at the end of this Student Guide.*

An FCL can never be granted to a contractor under FOCI.

- True
- False

FOCI has no impact on a contractor's eligibility for an FCL.

- True
- False

FOCI can be mitigated to allow a contractor an FCL.

- True
- False

## **Conclusion**

### ***Lesson Summary***

You have completed the FOCI and the FCL lesson.

## Answer Key

### Review Activity 1

A U.S. company is considered to be operating under FOCI when a foreign interest has \_\_\_\_\_ to make decisions that may compromise classified information.

- Direct power (correct response)
- Indirect power (correct response)
- Exercised power (correct response)
- Unexercised power (correct response)

**Feedback:** All of these apply. It does not matter whether the foreign interest has direct or indirect power or whether it can exercise that power—the company is still considered under FOCI.

### Review Activity 2

An FCL can never be granted to a contractor under FOCI.

- True
- False (correct response)

**Feedback:** The FOCI may be of a source, nature, and extent that is unlikely to have an adverse effect on national security, and therefore, the contractor may be granted an FCL.

FOCI has no impact on a contractor's eligibility for an FCL.

- True
- False (correct response)

**Feedback:** FOCI must be assessed to determine if granting the contractor an FCL would be inconsistent with national security interests.

FOCI can be mitigated to allow a contractor an FCL.

- True (correct response)
- False

**Feedback:** Even if a contractor is determined to be under FOCI, security measures can be put into place that will allow the contractor to be granted an FCL.

Student Guide

# Clearances in Industrial Security: Putting It All Together

---

## *Lesson 5: Course Conclusion*

### Contents

Course Conclusion .....	2
Course Summary .....	2
Lesson Review .....	2
Course Objectives .....	2

## Course Conclusion

### **Course Summary**

In this course, you learned about the purpose of facility security clearances (FCLs) and personnel security clearances (PCLs), the levels at which they are granted, the process for obtaining each, and how they are related. You also learned about foreign ownership, control, or influence (FOCI) and how it affects a company's FCL.

### **Lesson Review**

Here is a list of lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: FCL and PCL Overview
- Lesson 3: FCL and PCL Processes and Relationships
- Lesson 4: FOCI and the FCL
- Lesson 5: Course Conclusion

### **Course Objectives**

Congratulations. You have completed the Clearances in Industrial Security: Putting It All Together course.

You should now be able to:

- Identify the purpose of an FCL and a PCL
- Identify what is required for an individual to obtain a PCL
- Identify the elements for obtaining an FCL
- Identify how FCLs and PCLs are related
- Identify the effect of FOCI on an FCL

To receive credit for this course, you must take the *Clearances in Industrial Security: Putting It All Together* examination.

## Glossary

# Clearances in Industrial Security: Putting It All Together

---

**Access:** The ability and opportunity to gain knowledge of classified information.

**Adjudicative Guidelines:** Guidelines used to determine eligibility for access to classified information or assignment to sensitive duties. There are 13 adjudicative guidelines used to make eligibility determinations.

**Business Structure:** Organization framework legally recognized in a particular jurisdiction for conducting commercial activities, such as sole proprietorship, partnership, and corporation.

**Classified Contract:** Any contract requiring access to classified information by a contractor in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.) The requirements prescribed for a “classified contract” also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other GCA program or project which requires access to classified information by a contractor.

**Classified Information:** Official information that has been determined, pursuant to Executive Order 12958 or any predecessor order, or pursuant to the Atomic Energy Act of 1954, to require protection against unauthorized disclosure in the interest of national security which has been designated.

**Clearance:** An administrative authorization for access to National Security Information (NSI) up to a stated classification level (TOP SECRET, SECRET, CONFIDENTIAL).

**Cleared Company:** A contractor that has been granted FCLs and all contractor facilities being processed for an FCL.

**Cleared Employees:** All contractor employees granted PCLs and all employees being processed for PCL.

**Cognizant Security Agencies (CSAs):** Agencies of the Executive Branch that have been authorized by Executive Order 12829 to establish an industrial security program to safeguard classified information under the jurisdiction of these agencies when disclosed or released to U.S. industry. These agencies are: The Department of Defense, Office of

the Director of National Intelligence, Department of Energy, Nuclear Regulatory Commission, and Department of Homeland Security.

**Commercial and Government Entity (CAGE) Code:** A five position code that identifies companies doing or wishing to do business with the federal government. The first and fifth positions in the code must be numeric. The third and fourth positions may be any mixture of alpha/numeric excluding I and O. The code is used to support a variety of mechanized systems throughout the government.

**CONFIDENTIAL:** The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.

**Contract Security Classification Specification (DD 254):** DD Form 254 provides to the cleared contractor or cleared subcontractor the security requirements and the classification guidance that are necessary to perform on a specific classified contract.

**Contractor:** Any industrial, educational, commercial, or other entity that has been granted an FCL by a CSA.

**DD Form 254:** *see Contract Security Classification Specification*

**DD Form 441:** *see Department of Defense (DoD) Security Agreement*

**Defense Office of Hearings and Appeals (DOHA):** Determine whether an applicant's request for access to classified information is clearly consistent with the national interest to grant or continue security eligibility for the applicant.

**Defense Security Service (DSS):** An agency of the Department of Defense (DoD) located in Quantico, Virginia with field offices throughout the United States. The Under Secretary of Defense for Intelligence provides authority, direction, and control over DSS. DSS provides the military services, defense agencies, 30 federal agencies, and approximately 13,500 cleared contractor facilities with security support services. DSS is the CSO for most DoD classified contracts.

DSS supports the National Security and the warfighter, secures the nation's technological base, and oversees the protection of U.S. and foreign classified information in the hands of industry. DSS accomplishes this mission by clearing industrial facilities, accrediting information systems, facilitating the personnel security clearance process, delivering security education and training, and providing information technology services that support the industrial and personnel security missions of DoD and its partner agencies.

**Defense Security Service, Center for Development of Security Excellence (CDSE):**

Responsible for providing security education and training to DoD and other U.S. government personnel, DoD contractors, and sponsored representatives of foreign governments.

**Defense Security Service, Facility Clearance Branch (FCB):** Processes contractors for facility security clearances (FCLs) based upon procurement need, issues FCLs, and monitors the contractor's continued eligibility in the NISP.

**Defense Security Service, Foreign Ownership, Control, or Influence (FOCI) Office:**

Works with the local IS Rep to resolve issues that arise when a cleared facility or a facility being processed for a facility clearance is subject to foreign ownership, control, or influence.

**Defense Security Service, Industrial Security Representative (IS Rep):** Local representative from the Defense Security Service that provides advice and assistance to cleared contractors on security matters and with establishing a security program to ensure the facility is in compliance with the NISP.

**Defense Security Service, Personnel Security Management Office for Industry (PSMO-I):** Processes requests for and other actions related to personnel security clearances for personnel from facilities participating in the NISP.

**Defense Security Service, Special Programs:** Manages the security oversight function of DSS's direct and indirect support to the Special Access Program (SAP) community.

**Department of Defense (DoD):** The largest Cognizant Security Agency (CSA) with the most classified contracts with industry.

**Department of Defense Consolidated Adjudicative Facility (DoD CAF):** Responsible for issuing a clearance authorization for eligible individuals.

**Department of Defense (DoD) Security Agreement (DD 441):** A Department of Defense Security Agreement that is entered into between a contractor who will have access to classified information and the DoD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information.

**DOHA:** *see Defense Office of Hearings and Appeals*

**e-FCL:** *see Electronic Facility Clearance System*

**e-QIP:** *see Electronic Questionnaires for Investigations*

**Electronic Facility Clearance System (e-FCL):** System that all companies must use while in process for a facility clearance or to report a changed condition.



**Electronic Questionnaires for Investigations (e-QIP):** An Office of Personnel Management (OPM) software program for the preparation and electronic submission of security forms for a Personnel Security Investigation (PSI) or suitability determination.

**Eligibility:** The DoD Consolidated Adjudication Facility (DoD CAF) has made an adjudicative determination of member's Personnel Security Investigation (PSI) and that member may have access to classified information equal to the level of their adjudicated investigation.

**Facility:** A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined herein.) For the purposes of industrial security, the term does not include government installations.

**Facility Security Clearance (FCL):** An administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories).

**Facility Security Officer (FSO):** A U.S. citizen employee appointed by a contractor who will supervise and direct security measures necessary for implementing the NISPOM and other federal requirements for classified information.

**FCL Orientation Handbook:** Provides guidance to the Facility Security Officer on the facility security clearance (FCL) process, including business structure and excluded tier entities, the e-FCL process, accounts and systems and preparing for the initial review.

**Foreign Interest:** Any government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered, or incorporated under the laws of any country other than the United States or its territories; and any person who is not a citizen or national of the United States.

**Foreign Ownership, Control, or Influence (FOCI):** Whenever a foreign interest has the power—direct or indirect, whether or not exercised, and whether or not exercisable—to direct or decide matters affecting the management or operations of a company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

**Government Contracting Activity (GCA):** An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

**Industrial Security:** That portion of information security concerned with the protection of classified information in the custody of U.S. industry.

**Investigation:** The action of investigating something or someone; formal or systematic examination or research.

**Investigative Service Provider (ISP):** An entity that performs background investigations. The ISP for DoD is the Office of Personnel Management (OPM).

**Joint Personnel Adjudication System (JPAS):** The DoD system of record for contractor eligibility and access for personnel security clearances.

**JPAS:** *see Joint Personnel Adjudication System*

**Key Management Personnel (KMP):** Senior management identified in a facility that require an eligibility determination in order for a facility to be granted a facility clearance.

**National Industrial Security Program (NISP):** Established by Executive Order 12829 for the protection of classified information released or disclosed to industry in connection with classified contracts. The NISP applies standards for the protection of classified information released or disclosed to contractors of all federal executive branch departments and agencies. Requirements of the NISP are stated in the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M.

**National Security:** Encompasses both the national defense and the foreign relations of the U.S. Every nation must be able to defend itself, to ensure its own survival and the survival of its way of life. This ability of our nation to defend itself is one aspect of national security. Another way a nation can defend itself is to maintain a good working relationship with other countries, thereby reducing the threat to our nation's survival. For this reason, foreign relations are also part of how we define national security.

**Office of Personnel Management (OPM):** Provides investigation support for personnel clearances and sponsors the Extranet for Security Professionals online forum.

**OPM:** *see Office of Personnel Management*

**Personnel Security Clearance (PCL):** An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

**SECRET:** The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.

**Security Training, Education, and Professionalization Portal (STEPP):** The learning management system used by the Center for Development of Security Excellence (CDSE). STEPP is where the list of courses is maintained and where student information and course transcripts are maintained.

**SAM Database:** *see System for Award Management Database*

**Secure Web Fingerprint Transmission (SWFT):** Web-based system that allows users to submit e-fingerprints and demographic information for personnel security clearance (PCL) applicants.

**Security Clearance Package:** Package submitted electronically for an initial investigation request. It consists of the Electronic Questionnaires for Investigations Processing (e-QIP), signature forms, and fingerprints via Secure Web Fingerprint Transmission (SWFT).

**Sensitive Compartmented Information (SCI):** Information that needs extra protection above a Top Secret security clearance level. SCI can come from various sources and has to have special handling, which involves controls to access.

**SF 328:** Certificate Pertaining to Foreign Interests.

**Special Access Program (SAP):** Any program that is established to control access and distribution and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A Special Access Program can be created or continued only as authorized by a senior agency official delegated such authority pursuant to the NISPOM.

**Sponsorship:** The contractor requiring an FCL cannot request a clearance on its own behalf, but instead must be supported (sponsored) by a government entity or by another cleared contractor that is procuring services requiring access to classified information from the uncleared contractor.

**Summary Data Sheet:** Document containing basic information about a facility such as the facility's website, stock information, and previous names.

**SWFT:** *see Secure Web Fingerprint Transmission*

**System for Award Management (SAM) Database:** Secure web portal that consolidates various government acquisition and award capabilities into one system.

**TOP SECRET:** The classification level applied to information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to National Security that the Original Classification Authority (OCA) is able to identify or describe.