

Student Guide

Clearances in Industrial Security: Putting It All Together

Lesson 1: Course Introduction.....	4
Introduction.....	4
Welcome.....	4
Roles	4
Course Objectives.....	5
Lesson 2: FCL and PCL Overview	6
Introduction.....	6
Objectives.....	6
Definitions, Purpose, and Levels.....	6
FCL and PCL Comparisons	6
Definition and Purpose	6
Levels.....	7
Scenario	8
Review Activities.....	9
Now check your knowledge.	9
Review Activity 1	9
Conclusion.....	10
Lesson Summary	10
Lesson 3: FCL and PCL Processes and Relationships.....	11
Objectives.....	11
Steps for Obtaining an FCL	11
Overview.....	11
Sponsorship.....	12
FCL Orientation Handbook	12
CAGE Code.....	12
Information Gathering	13
PCLs for KMP	15
Eligibility Determination.....	16
FCL Summary.....	17
Steps for Obtaining a PCL	17
Overview.....	17
Identification of Need-to-Know	18
Information Gathering	18
Package Reviews	18

Investigation.....	19
Adjudication	19
Eligibility Determination.....	23
PCL Summary	24
FCL/PCL Relationship	24
Relationships	24
Contingency	24
Classification Level.....	25
Review Activities.....	26
Review Activity 1.....	26
Review Activity 2.....	27
Review Activity 3.....	28
Conclusion.....	29
Lesson Summary	29
Lesson 4: FOCI and the FCL.....	30
Objectives.....	30
Definition	30
What Is FOCI?	30
FOCI Determination.....	30
Overview.....	30
FOCI Factors	31
Impact of FOCI on the FCL.....	31
FCL Eligibility.....	31
Eligibility Reassessment	31
Scenario	32
Review Activities.....	33
Now check your knowledge	33
Review Activity 1.....	33
Review Activity 2.....	33
Conclusion.....	34
Lesson Summary	34
Lesson 5: Course Conclusion.....	35
Course Summary	35
Lesson Review	35
Course Objectives.....	35
Lesson 2 Answer Key	36
Review Activity 1.....	36
Lesson 3 Answer Key	37
Review Activity 1.....	37
Review Activity 2.....	38

Review Activity 3.....	39
Lesson 4 Answer Key	40
Review Activity 1.....	40
Review Activity 2.....	40

Lesson 1: Course Introduction

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 classified contract, Ellen is correct that this does not mean they are automatically cleared to access classified information. A company must meet specific requirements for a favorable entity eligibility determination (also referred to as a Facility Clearance, or FCL) and applicable personnel must obtain a favorable national security eligibility determination (also referred to as a Personnel Security Clearance, or PCL). Some of these PCLs must be in connection with the FCL. But what clearances are needed? And who must be cleared? How are both obtained? How might Foreign Ownership, Control, or Influence, or 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

National security eligibility determinations to access 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 companies and individuals who will adequately protect this information.

In this course, you will learn how these roles work together to determine the eligibility for an FCL and PCL.

Course Objectives

Here are the course objectives:

- Identify the purpose of Facility and Personnel Security Clearances
- Identify the requirements for a Personnel Security Clearance
- Identify the elements for obtaining a Facility Clearance
- Identify the association between Facility and Personnel Security Clearances
- Identify the impact of Foreign Ownership, Control, or Influence on a facility's clearance

Lesson 2: FCL and PCL Overview

Introduction

Objectives

The National Industrial Security Program, or 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 classification levels at which they are granted.

Here are the lesson objectives:

- Identify the purpose of Facility and Personnel Security Clearances
- Identify the classification levels granted for a Facility Clearance
- Identify the classification levels granted for a Personnel Security Clearance

NISP

National Industrial Security Program

Definitions, Purpose, and Levels

FCL and PCL Comparisons

FCLs and PCLs are closely connected 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 associated with 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.

FCL

Facility Clearance

PCL

Personnel Security Clearance

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 FOCI and whether it can be mitigated.

A PCL is 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.

Both FCLs and PCLs are determinations for eligibility to classified information.

FCLs are granted to companies, meaning that the Key Management Personnel, or KMP, who have the authority to directly or indirectly plan and control business operations have been appropriately cleared, in addition to meeting other administrative requirements.

The KMP of a facility must include the Senior Management Official, or SMO, the Facility Security Officer, or FSO, and the Insider Threat Program Senior Official, or ITPSO.

PCLs are granted to individuals, such as employees who have a need to access classified information or KMP in connection with the FCL.

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.

Levels

FCLs and PCLs are granted at the Confidential, Secret, and Top Secret classification levels. A cleared company or cleared individual is only authorized to access classified information at the same or lower classification level of eligibility granted. A cleared employee's classified access is limited by their company's FCL level. For example, if an employee has an active Top Secret PCL eligibility and their company's FCL is only at the Secret level, the employee may only access classified information at the Secret level while performing classified work for that company. In some cases, companies will require additional accesses and eligibility criteria. For example, when a classified contract requires access to a Special Access Program, or SAP, or Sensitive Compartmented Information, or 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.

FCL

Facility Clearance

PCL

Personnel Security Clearance

Scenario

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

First, Johnson Technology Services will need an FCL. KMP and employees who will support the contract that require access to classified information will need PCLs. Since information must be accessed at the same or lower classification level of eligibility granted, the FCL and any PCLs required in support of the contract will need to be at the Secret level.

FCL

Facility Clearance

PCL

Personnel Security Clearance

KMP

Key Management Personnel

Review Activities

Now check your knowledge.

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 Clearance (FCL)
- Personnel Security Clearance (PCL)
- Both FCL and PCL

Question 2 of 3. Which of the following is an administrative determination that an individual 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 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 Clearance (FCL)
- Personnel Security Clearance (PCL)
- Both FCL and PCL

Conclusion

Lesson Summary

You have completed the FCL and PCL Overview lesson.

Lesson 3: FCL and PCL Processes and Relationships

Introduction

Objectives

Before Johnson Technology Services can access the classified information necessary to fulfill its contractual obligations, it will need to receive an FCL and its KMP and staff will need PCLs.

In this lesson, you will learn the process for obtaining an FCL and PCL, and the relationship between them.

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

- Identify the FCL process
- Identify a company's eligibility requirements for an FCL
- Identify the PCL process
- Identify an individual's eligibility requirements for a PCL
- Identify how an FCL is contingent upon applicable PCLs
- Identify the limitations of classified access per FCL and PCL levels

FCL

Facility Clearance

PCL

Personnel Security Clearance

Steps for Obtaining an FCL

Overview

Obtaining an FCL is a multi-step process.

First, a company must be sponsored for an FCL based upon a need to access classified information.

Once the Defense Counterintelligence and Security Agency, or DCSA, receives and validates the FCL sponsorship request, the company's FSO will be notified electronically, initiating the process with certain deadlines and instructions. The notification may identify other resources the FSO is encouraged to review for guidance on the FCL process as well.

If the company does not already have a Commercial and Government Entity or CAGE Code, one must be obtained prior to FCL issuance.

The company must provide certain information about itself in the FCL system of record and applicable KMP must obtain PCLs or be formally excluded from access to classified information.

Finally, in accordance with national security adjudicative guidelines, an eligibility determination will be made.

Let's 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 currently cleared to participate in the NISP or a Government Contracting Activity, or GCA, when a definite classified procurement need to access classified information has been established.

The FCL sponsorship is initiated in the FCL system of record through a system-generated FCL sponsorship request. The sponsorship package must include justification demonstrating a bona fide procurement requirement to access classified information. The most common form used to support this need is the DD Form 254, DoD Contract Security Classification Specification.

Written GCA or Intelligence Community, or IC, authorization is required, and it is highly recommended that a contract or subcontract specific Statement of Work, or SOW, or Performance Work Statement, or PWS, also be included in the package.

GCA

Government Contracting Activity

FCL

Facility Clearance

FCL Orientation Handbook

The FCL Orientation Handbook provides guidance on the FCL process, including FSO responsibilities, business structure and excluded tier entities, accounts and systems, critical deadlines, and other detailed information about the FCL process.

Contractors are encouraged to review and be familiar with the guidance provided in this handbook.

FSO

Facility Security Officer

FCL

Facility Clearance

CAGE Code

DCSA 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, or SAM, database.

CAGE

Commercial and Government Entity

FCL

Facility Clearance

Information Gathering

The company's FSO will work with the DCSA to determine which forms must be uploaded in the FCL system of record. While this varies based on business and management structure, all companies must submit:

- The SF-328, the Certificate Pertaining to Foreign Interests
- A summary of basic information about the company, such as the company's website, stock information, and previous names
- Corporate governance documents
- Organizational chart
- Specific information for 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.

KMP

Key Management Personnel

FSO

Facility Security Officer

DCSA

Defense Counterintelligence and Security Agency

NOTE: The information in the Forms Required section 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 DCSA 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 FCL system of record
- Provide all supplemental responses to affirmative SF 328 questions

Company Summary

- 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 Information

- 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 DCSA 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 FCL system of record upon receipt of countersignatures from DCSA

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, applicable KMP must first be cleared. Which KMP are required to be cleared is based on the business and management structures and organization of the facility.

The DCSA Industrial Security Representative, or IS Rep, can help identify and determine KMP who must be cleared and KMP who may be excluded. The company must submit exclusion resolutions for excluded KMP. DCSA will initiate the PCL process for KMP who must be cleared in connection with the FCL.

IS Rep

Industrial Security Representative

NOTE: The information in the KMP Requiring PCLs section 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
- Insider Threat Program Senior Official (ITPSO), if other than the SMO or FSO

General Partnership

- SMO
- FSO
- ITPSO
- All general partners, except:
 - Single Partner (must be cleared)
 - Management Committee (all committee members must be cleared)

Limited Partnership

- SMO
- FSO
- ITPSO
- All general partners except:
 - Single Partner (must be cleared)
 - Management Committee (all committee members must be cleared)
 - Limited Partners need PCLs if they work on classified contracts or need access to classified information

Limited Liability Company (LLC)

- SMO
- FSO

- ITPSO
- All LLC members must be cleared or excluded
 - Eligibility for classified access depends on the members' 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
- ITPSO
- Chief Executive Officer (CEO)
- Other officers/officials with accountability for classified contracts
- All regents/trustees/directors, except:
 - 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 in accordance with the NISPOM.

Eligibility Determination

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

- First, the company must require access to the classified information in connection with a legitimate U.S. Government or foreign government requirement and access must be consistent with U.S. national security interests as determined by the CSA.
- 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 fifty states, the District of Columbia, an organized U.S. territory, 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 or agreements.
- The company must not be under FOCl to such a degree that the granting of the FCL would be inconsistent with national security interests, and it must not pose an unacceptable risk to national security interests.
- Finally, the company must meet all CSA or government-wide policy requirements for access to the type of classified information or program involved.

DCSA may issue an interim FCL with IS Rep concurrence when all requirements have been met and applicable KMP have been granted the same level or higher interim PCLs. After an FCL is granted, the company must continue to meet all eligibility requirements and report any change in conditions that may impact it.

FOCI

Foreign Ownership, Control, or Influence

FCL Summary

Now that you've seen the process for obtaining an FCL, think for a moment about what Ellen must 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 in performance of the contract.

First, the sponsoring GCA or currently cleared company must submit the sponsorship letter and proof of contractual need to DCSA via the FCL system of record.

Once the sponsorship is validated, the company FSO will receive the acceptance via an electronic notification from DCSA, initiating the FCL process. Important information with next steps and critical deadlines about the FCL process will be provided as well.

The FCL Orientation Handbook is a valuable resource the FSO is encouraged to review.

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 in the FCL system of record.

Ellen must work with her company's IS Rep to determine which KMP will need PCLs and which KMP can be excluded before a determination will be made.

If you would like to learn more about FCLs, refer to the Facility Clearances in the NISP eLearning course available through the CDSE website.

Steps for Obtaining a PCL

Overview

Obtaining a PCL is a multi-step process.

It begins when a cleared company determines and verifies an employee will require access to classified information in performance of a classified contract.

The FSO will initiate the clearance request process via the DoD Personnel Security System of Record. When a company is in the process of obtaining an FCL, the DCSA initiates the PCL process for KMP.

The employee must provide information about him- or herself by completing a security questionnaire; then, the security clearance package must be reviewed for

completeness and adequacy by the FSO prior to releasing it to DCSA for vetting.

A national security background investigation is conducted on the employee, and the results of the investigation are reviewed and considered in accordance with national security adjudicative guidelines to reach an eligibility determination.

Identification of Need-to-Know

Once a determination is verified that an employee will require access to classified information in performance of tasks or services related to the fulfillment of a classified contract, the PCL process is initiated.

A PCL must not be initiated for an individual unless the individual is associated with a cleared company and a need for classified access has been determined.

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 via the DoD Personnel Security System of Record. If the employee's record shows a clearance as active, the company will need to assume ownership and determine if a background investigation is required before proceeding. If the employee requires an upgrade to the level of a current PCL, has never held a PCL, or previous access to classified information has been inactive for more than 24 months, this is referred to as an initial clearance.

FSO

Facility Security Officer

PCL

Personnel Security Clearance

Information Gathering

There are key security forms the employee must submit electronically for an initial clearance request:

- The completed security questionnaire
- Signature on a certification and all appropriate release forms
- A current set of fingerprints uploaded via an approved secure transmission system

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

Package Reviews

The FSO informs the employee in writing that the security package will be reviewed for adequacy and completeness only, and the information will be used for no other purpose within the company.

After the employee completes, signs, and electronically submits the security

clearance questionnaire, the FSO will review all of the forms before releasing the security clearance package in the DoD personnel security system of record to DCSA for vetting.

DCSA vets the security package, then forwards it to the Investigative Service Provider, or ISP. For DoD, the ISP is also DCSA. While vetting the security clearance package, DCSA will make an interim PCL determination and update the DoD personnel security system of record accordingly.

In some cases, employees may be allowed to work with an interim clearance, provided the company has at least an interim FCL.

FSO

Facility Security Officer

Investigation

The ISP also reviews the security clearance package prior to opening the national security background investigation. If the package is incomplete, the ISP will coordinate with the FSO—or the appropriate governmental branch, in the case of a company in-process for an FCL—to resolve any issues. Once the ISP completes the investigation, the results are submitted to the DoD CAF for eligibility determination.

ISP

Investigative Service Provider

FSO

Facility Security Officer

DoD CAF

Department of Defense Consolidated Adjudications Facility

Adjudication

The DoD CAF determines a final eligibility in accordance with the Office of the Director of National Intelligence, or ODNI, and the Security Executive Agent Directive, or SEAD 4 National Security Adjudicative Guidelines.

You may also learn more about each of the adjudicative guidelines through the Personnel Security Shorts available on the CDSE website.

DoD CAF

Department of Defense Consolidated Adjudications Facility

NOTE: The information in the National Security Adjudicative Guidelines section below will not be on the test but is included here as additional information that may provide useful background information and insight.

National Security Adjudicative Guidelines

Allegiance to the United States

An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified or sensitive information is in doubt if there is any reason to suspect an individual's allegiance to the United States. Negative indicators include participation in or support for acts against the United States or placing the welfare or interests of another country above those of the United States.

Example: Involvement, association, or sympathy with persons in an organization that supports the overthrowing of the U.S. Government.

Foreign Influence

Foreign contacts and interests, including, but not limited to, business, financial, and property interests, are a national security concern if they result in divided allegiance. They may also be a national security concern if they create circumstances in which the individual may be manipulated or induced to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or otherwise made vulnerable to pressure or coercion by any foreign interest.

Example: Failure to report or fully disclose, when required, association with a foreign person, group, government, or country.

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 provide information or make decisions that are harmful to the interests of the United States.

Example: Failure to use a U.S. passport when entering or exiting the U.S.

Sexual Behavior

Sexual behavior that involves a criminal offense; reflects a lack of judgement or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgement, reliability, trustworthiness, and ability to protect classified or sensitive information. No adverse inference concerning the Guidance standards may be raised solely on the basis of the sexual orientation of the individual.

Example: Sexual behavior of a criminal nature, whether or not the individual has been prosecuted.

Personal Conduct

Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

Example: Subject left previous employment due to fraud.

Financial Considerations

Failure to live within one's means, satisfy debts and meet financial obligations may indicate poor self-control, lack of judgement, or unwillingness to abide by rules and regulations. All of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. An individual who is financially overextended is at risk of having to engage in illegal or otherwise questionable acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts, including espionage.

Example: A history of not meeting financial obligations or an inability or unwillingness to satisfy debts regardless of the ability to do so.

Alcohol Consumption

Excessive alcohol consumption often leads to the exercise of questionable judgment, or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.

Example: Alcohol-related incidents away from or at work, such as driving while under the influence; reporting to work in an intoxicated or impaired condition.

Drug Involvement and Substance Misuse

The illegal use of controlled substances, to include the misuse of prescription and non-prescription drugs, and the use of other substances that cause physical or mental impairment or are used in a manner inconsistent with their intended purpose can raise questions about an individual's reliability and trustworthiness, both because such behavior may lead to physical or psychological impairment and because it raises questions about a person's ability or willingness to comply with laws, rules and regulations.

Example: Any substance misuse; testing positive for an illegal drug;

illegal drug possession.

Psychological Conditions

Certain mental and personality conditions can impair judgement, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference concerning the Guidance standard may be raised solely on the basis of mental health counseling.

Example: Behavior that casts doubt on an individual's judgement, stability, reliability, or trustworthiness; pathological gambling; mental or personality condition, including but not limited to, violent, self-harm, deceitful, exploitative, or bizarre behaviors.

Criminal Conduct

Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules, and regulations.

Example: A pattern of offenses, regardless of whether the individual was formally charged, prosecuted, or convicted, felony convictions, or imprisonment for over one year.

Handling Protected Information

Deliberate or negligent failure to comply with rules and regulations for handling protected information, which includes classified and other sensitive government information, and proprietary information raises doubts about an individual's trustworthiness, judgement, reliability, or willingness, and ability to safeguard such information, and is a serious security concern.

Example: Deliberate or negligent disclosure of protected information to unauthorized persons, multiple security violations.

Outside Activities

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

Example: employment or service with a foreign country or foreign national.

Use of Information Technology

Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness, or ability to properly protect sensitive systems, networks, and information. Information technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information.

Example: Unauthorized entry into any information technology system; downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system.

Eligibility Determination

Each case is judged on its own merits. The DoD CAF makes an eligibility determination, and if favorable, classified access is granted to the employee by the company.

Any doubt regarding whether access to classified information is clearly consistent with the national security interests of the U.S. 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 national 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, or DOHA, to determine whether it is clearly consistent with the national security interests of the U.S. to grant or continue national security eligibility for the employee.

DOHA

Defense Office of Hearings and Appeals

PCL

Personnel Security Clearance

DoD CAF

Department of Defense Consolidated Adjudications Facility

PCL Summary

Now that you've seen the process for obtaining a PCL, think for a moment what must be done for an employee of Johnson Technology Services who will need access to classified information in support of the company's new classified contract.

Once the FSO at Johnson Technology Services has verified that the employee requires access to classified information, the FSO must determine if the employee holds an active clearance or has in the past 24 months and, if not, the FSO will initiate the clearance request process via the DoD Personnel Security system of record.

The employee must electronically complete the security questionnaire, digitally sign the certification, and appropriate release forms, and a set of fingerprints must be captured and uploaded via a secure transmission system.

The security clearance package is released in the DoD Personnel Security System of Record by the FSO to DCSA for vetting and interim clearance determination.

The ISP conducts the national security background investigation and provides all the collected information to the DoD CAF. At this point, the DoD CAF determines a final eligibility in accordance with national security adjudicative guidelines based on review and consideration from results and other available, reliable information collected from the national security background investigation.

If the DoD CAF cannot favorably find that it is clearly consistent with the national interest to make a final eligibility determination, the case is referred to DOHA for further processing and/or where the case will be decided before an Administrative Judge.

If you would like to learn more about PCLs, refer to the Personnel Clearances in the NISP eLearning course available through the CDSE website.

FCL/PCL Relationship

Relationships

FCLs and PCLs are connected in two ways. Eligibility for an FCL is contingent on essential KMP obtaining and maintaining PCL favorable eligibility determination. FCLs and PCLs also impact the level of classified material that can be handled.

Contingency

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

Classification Level

Keep in mind that a facility must 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. If the company's FCL and an employee's PCL are at different levels, this difference will have an impact on both.

For example, if an employee has a Top Secret PCL and works for a company with a Secret FCL, the employee can only access information at the Secret classification level or below while performing classified work for that company.

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

Review Activities

Review Activity 1

Now, check your knowledge

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

Try this activity.

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
- DCSA
- ISP
- DoD CAF

Makes the final eligibility determination

- FSO
- DCSA
- ISP
- DoD CAF

Conducts the national security background investigation

- FSO
- DCSA
- ISP
- DoD CAF

Initiates the clearance process

- FSO
- DCSA
- ISP
- DoD CAF

Review Activity 3

Answer this question.

When is FCL eligibility contingent 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.

Lesson 4: FOCI and the FCL

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 an FCL, it is important to assess whether 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. Take a moment to review them.

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

FOCI

Foreign Ownership, Control, or Influence

FCL

Facility Clearance

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

Foreign Ownership, Control, or Influence

FOCI Determination

Overview

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

CAGE

Commercial and Government Entity

PCL

Personnel Security Clearance

KMP

Key Management Personnel

FOCI Factors

When making a FOCI determination, DCSA considers several factors in the aggregate relating to the company, the foreign interest, and the government of the foreign interest as appropriate. Please take a moment to review these factors.

- Record of economic and government espionage against U.S. targets
- Record of enforcement and/or engagement in unauthorized technology transfer
- The type and sensitivity of the information that shall be accessed
- The source, nature, and extent of FOCI, including if:
 - Foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies
 - A minority position consists of greater than 5% of the ownership interest or greater than 10% of the voting interests
- Record of compliance with pertinent U.S. laws, regulations, and contracts
- The nature of any bilateral and multilateral security and information exchange agreements that may pertain
- Ownership or control, in whole or in part, 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. A currently cleared company's FCL may continue to exist when determined to be under FOCI when negotiating an acceptable FOCI mitigation or negation measure, if there is no indication that classified information is at risk or compromise.

If acceptable security measures are not taken to prevent unauthorized access or adverse effects on classified contracts, an existing FCL will be invalidated or revoked.

To learn more about the FOCI determination process and FOCI mitigation plans, refer to the Understanding FOCI eLearning course and the FOCI Short available on the CDSE website.

FCL Eligibility***Eligibility Reassessment***

DCSA 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 company is operating or, alternatively, require amendments to the FOCI mitigation or negation agreement.

Depending on changed conditions, DCSA may determine that a company is no longer under FOCI or, conversely, that a company is no longer eligible for an FCL.

If a company does not have a current or pending requirement for access to classified information, DCSA will administratively terminate the FCL.

Scenario

“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. DCSA 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.

DCSA 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

Now check your knowledge.

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 company under FOCI.

- True
- False

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

- True
- False

FOCI can be mitigated to allow a company an FCL.

- True
- False

Conclusion

Lesson Summary

You have completed the FOCI and the FCL lesson.

Lesson 5: Course Conclusion

Course Conclusion

Course Summary

In this course, you learned about the purpose of FCLs and PCLs, the levels at which they are granted, the process for obtaining each, and how they are related. You also learned about FOCI and the impact it may have on 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 PCL
- Identify the requirements for a PCL
- Identify the elements for obtaining an FCL
- Identify the association between FCLs and PCLs
- Identify the impact of FOCI on an FCL

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

Lesson 2 Answer Key

Review Activities

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

- Facility Clearance (FCL) (correct response)
- Personnel Security Clearance (PCL)
- Both FCL and PCL

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

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

- Facility Clearance (FCL)
- Personnel Security Clearance (PCL) (correct response)
- Both FCL and PCL

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

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

- Facility 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.*

Lesson 3 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 a currently cleared company or a 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 DCSA 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, an organized U.S. territory, or a formally acknowledged American Indian or Alaska Native tribe.

Review Activity 2

Question 1 of 4. Determines eligibility for an interim clearance

- FSO
- DCSA (correct response)
- ISP
- DoD CAF

Feedback: *The DCSA determines if an individual is eligible for an interim clearance while vetting the security clearance package.*

Question 2 of 4. Makes the final eligibility determination

- FSO
- DCSA
- ISP
- DoD CAF (correct response)

Feedback: *The DoD CAF (or DOHA, if applicable) determines a final eligibility in accordance with national security adjudicative guidelines based on review and consideration from results and other available, reliable information collected from a national security background investigation.*

Question 3 of 4. Conducts the investigation

- FSO
- DCSA
- ISP (correct response)
- DoD CAF

Feedback: *The ISP conducts the national security background investigation after reviewing the security clearance package.*

Question 4 of 4. Initiates the clearance process

- FSO (correct response)
- DCSA
- ISP
- DoD CAF

Feedback: *The company's FSO initiates the process by submitting a clearance request using the DoD personnel security system of record.*

Review Activity 3

When is FCL eligibility contingent 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 is contingent on applicable KMP successfully obtaining PCLs.*

Lesson 4 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 to be under FOCI.

Review Activity 2

An FCL can never be granted to a company 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 company may be granted an FCL.

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

- True
- False (correct response)

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

FOCI can be mitigated to allow a company an FCL.

- True (correct response)
- False

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