

LESSON 4

Personnel Security Clearances General Concepts

In this lesson we'll examine the Industrial Personnel Security Clearance Program. This is a program to "clear" employees at industrial facilities for access to classified information when they need access to do their jobs. We will look briefly at who determines clearances and on what grounds. There will also be a section on what the FSO, can do to prevent delays in the clearance process. Finally, we will discuss the ways in which a clearance may be terminated.

OBJECTIVES

When you finish this lesson you should be able to do the following:

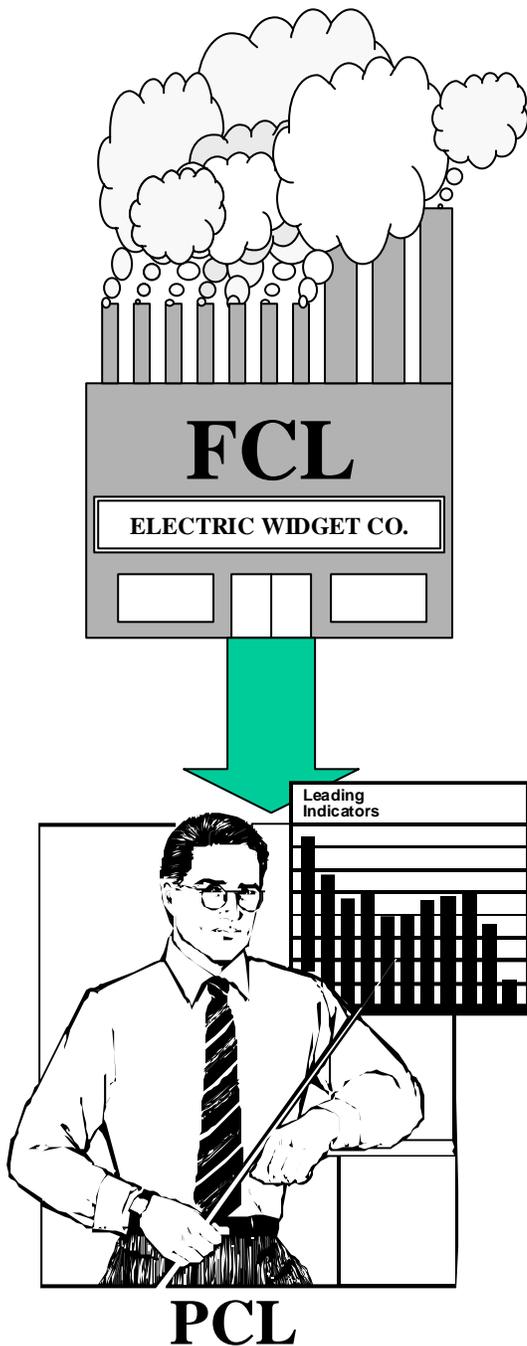
- Define a Personnel Security Clearance (PCL).
- Explain briefly the roles of the Defense Security Service, DISCO and the Defense Office of Hearings and Appeals (DOHA) in the granting, revocation, and denial of PCLs.
- Describe the general criteria for granting PCLs.
- Explain the ways in which you, the FSO, may aid in the process of clearing employees at your company.
- Differentiate clearance denial, suspension, revocation, and termination.

PERSONNEL SECURITY CLEARANCES

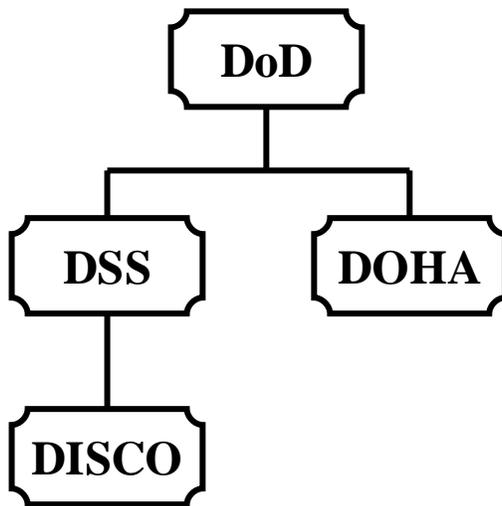
In the last lesson we discussed the reasons and procedures for the granting of Facility Security Clearances (FCL). One of the main reasons for a FCL was, however, touched upon lightly. That reason is people. A Facility Security Clearance is granted to allow the clearing of employees who have a need to handle classified information, either in the facility itself, at another cleared facility, or at a government installation. Where necessary, the approval of a facility for storage of classified information may be granted.

What is a Personnel Security Clearance? A Personnel Security Clearance (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 PCL being granted" (**Appendix C, NISPOM**). In other words, a PCL is ***a determination or prediction that an individual can be relied on to safeguard our national secrets.***

This is an important concept. The Personnel Security Clearance is not a piece of paper. It is a determination, essentially an educated guess, as to a person's character. And the issuance of a "final" clearance is *not* the final word on that person's character. The PCL philosophy allows for the possibility of inaccuracy in the original determination or prediction and also for the changes in a person's character over time. So continuing evaluation is called for. As part of this continuing evaluation, the government conducts periodic reinvestigations on cleared personnel. The level of the individual's clearance determines the frequency and depth of these investigations.



OGC and DOHA



Who makes the clearance determination or prediction? The determination is made by the Department of Defense at one of two levels. Favorable determinations may be made at the DSS *Defense Industrial Security Clearance Office (DISCO)* or, if further deliberation is required, the determination is made at the *Defense Office of Hearings and Appeals (DOHA)*. A favorable determination from either office prompts DISCO to issue an electronic *Letter of Consent (LOC)*, which informs the FSO that the applicant has been granted a clearance to a specified level. Again, this is not the clearance itself, only a notification. All denials and revocations of Personnel Security Clearances come from DOHA. DISCO is within the structure of the Defense Security Service. DOHA belongs to the DoD's Office of the General Counsel.

What is the clearance determination based on? The determination or prediction of the person's trustworthiness is based on some form of investigation. The nature and extent of the investigation is determined by the level of clearance required by the employee. There are three basic levels of classified information: **TOP SECRET**, **SECRET**, and **CONFIDENTIAL**. When an **Interim clearance** is granted to an employee, the access to classified information is more restrictive than a **FINAL Clearance** in terms of what information the holder is permitted to access. Interim **SECRET** and **CONFIDENTIAL** clearances granted by the Cognizant Security Agency (CSA) are valid for access to classified information at the level of the interim PCL. However, an Interim Clearance granted at the **SECRET** or **CONFIDENTIAL** level is not authorized for access to the following:

- Sensitive Compartmented Information
- Restricted Data (RD)
- COMSEC (Communications Security) Information
- SAP (Special Access Programs)
- NATO Information (See note on next page)

The Six Functions of DISCO

- Determine eligibility of applicants
- Initiate appropriate investigations
- Review investigative findings
- Refer doubtful cases to DOHA for adjudication
- Issue Letters of Consent (LOCs)
- Keep records of PCLs and

An interim **TOP SECRET Clearance** is valid for access to RD, COMSEC and NATO Information at the **SECRET and CONFIDENTIAL** level only.

NOTE: The following applies to NATO information:

Operation **ENDURING FREEDOM** has created a particular need to ensure timely access by involved operational commands and other activities to NATO classified. Accordingly, for the duration of **ENDURING FREEDOM**, contractor & military personnel with established need-to-know, that have been granted an interim PCL, are eligible for access to NATO information of the equivalent level of classification. Access to COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL information **is not authorized**. Access to NATO classified material for interim PCL's shall be subject to the following conditions:

- Approval by the authority who is granting access to U.S. classified information based on the interim security PCL.
- Written authorization, maintained as a record.
- Interim PCL held at the SECRET or TOP SECRET level
- Process for a final security clearance has been initiated
- Individual has received and acknowledged a briefing on NATO security requirements.

(As stated in the Office of the Under Secretary of Defense Memorandum, dated 4 Dec 01, SUBJECT: Facilitating Necessary Access to NATO Classified Information.)

Immigrant aliens and foreign nationals are not eligible for PCLs, but in special cases they may be granted a **Limited Access Authorization (LAA)** at the SECRET or CONFIDENTIAL level, as required. Many restrictions apply to LAAs; these restrictions are spelled out on charts in the next lesson.

PERSONNEL SECURITY INVESTIGATIONS



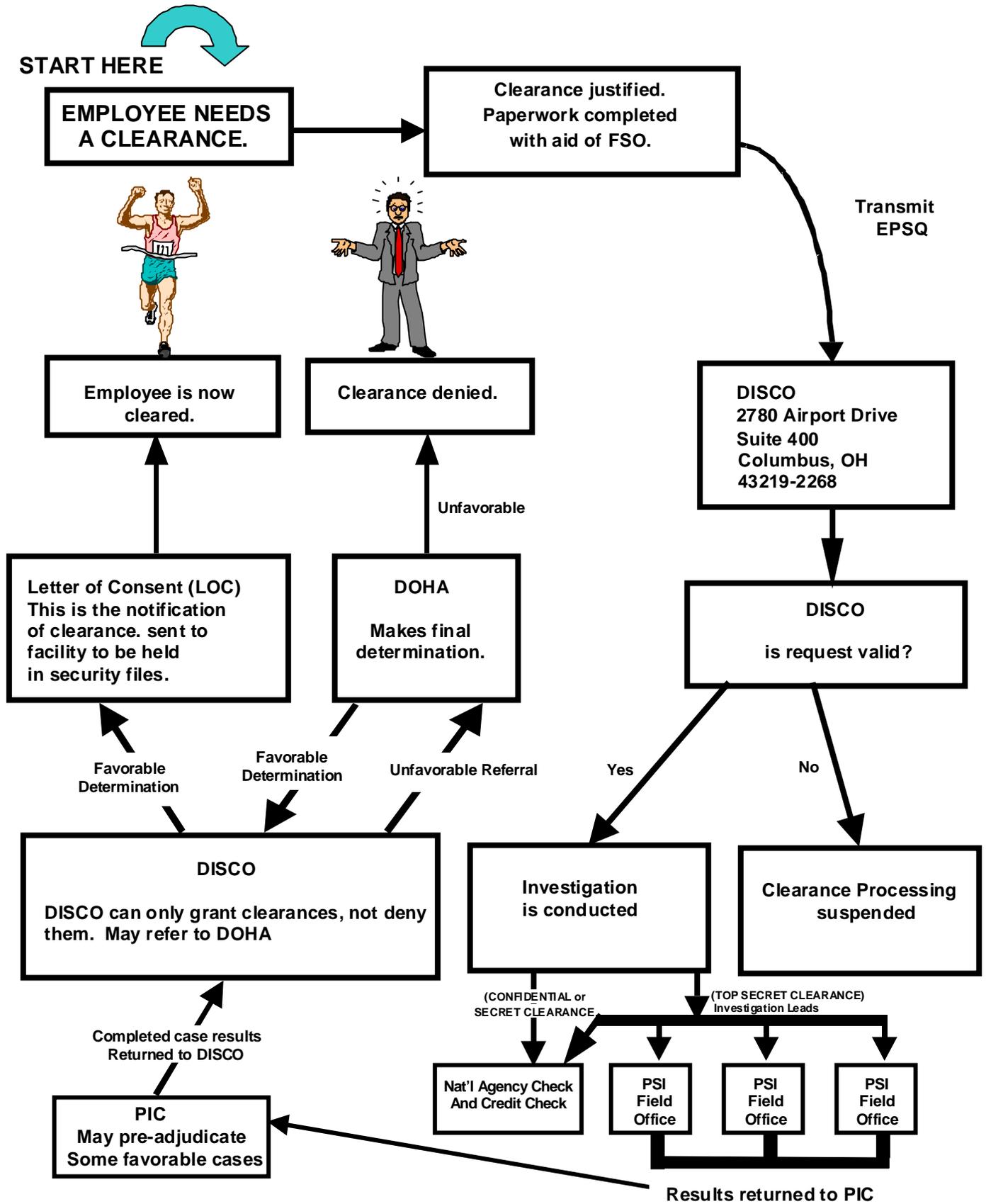
Special Agent's Badge



A National Agency Check with Local Agency Check and Credit Check (NACLC) is the basic investigative requirement for a SECRET or CONFIDENTIAL clearance. A Single Scope Background Investigation (SSBI) is required for a TOP SECRET clearance. Employees of the Defense Security Service or investigators representing the office of Personnel Management (OPM) carry out the actual investigations of applicants for clearances.

Essentially their job involves "running leads," that is, checking out references and records as indicated by the information on the Electronic Personnel Security Questionnaire (EPSQ) completed by the applicant for a security clearance. In many instances, they also conduct Subject Interviews with applicants.

LIFE CYCLE OF A PERSONNEL SECURITY INVESTIGATION



RIGHTS AND RESPONSIBILITIES OF CLEARED PERSONNEL

While being evaluated for a Personnel Security Clearance, an employee is entitled to the provisions of due process. These provisions, stated in Executive Order 12958, Access to Classified Information, mandate that a PCL cannot be denied or revoked unless an individual is given the following:

- A written explanation of the basis for the denial or revocation of the clearance.
- Any documents, records, and reports upon which the denial or revocation is based if they would be made available under the Freedom of Information Act or Privacy Act.
- An opportunity to be represented by legal counsel.
- A reasonable opportunity to reply to and request a review of the determination.
- Written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal.
- An opportunity to appeal in writing to a high level panel appointed by the agency head.
- An opportunity to appear personally at some point in the process before a government authority other than the investigating authority.

Bear in mind, no one has a right to a PCL. A person does have the right to a formal and impartial review of why a PCL is to be denied or revoked.

Along with the PCL the employee acquires the responsibility to protect classified information. *The employee learns the details of this protection through you, the FSO.* This knowledge comes through a number of methods: briefings, the SPP you may have prepared, memos, and many other ways. But ultimately, the responsibility rests with that employee. If the holder of a PCL is unable or unwilling to protect classified information, the NISP is undermined and national security threatened.

Personnel Security Clearance

Eligibility Criteria

Ideally, a person should not have a history of any of the following 13 activities and conditions, although a particular "involvement" will not necessarily be a basis for denial of clearance.

Guideline A: Allegiance to the United States

The Concern: 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.

Guideline B: Foreign influence

The Concern: 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.

Guideline C: Foreign preference

The Concern: 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.

Guideline D: Sexual behavior

The Concern: 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.

Guideline E: Personal conduct

The Concern: 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.

The Concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Guideline G: Alcohol consumption

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

Guideline H: Drug involvement

The Concern: 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.

Guideline I: Emotional, mental, and personality disorders

The Concern: 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. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Guideline J: Criminal conduct

The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Guideline F: Financial considerations

Personnel Security Clearance *Eligibility Criteria*

Guideline K: Security Violations

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Guideline L: Outside activities

The Concern: 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.

Guideline M: Misuse of Information Technology Systems

The Concern: 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.

These guidelines are published as Appendix A. of the Department of Defense (DoD) Personnel Security Regulation (DoD 5200.2R)

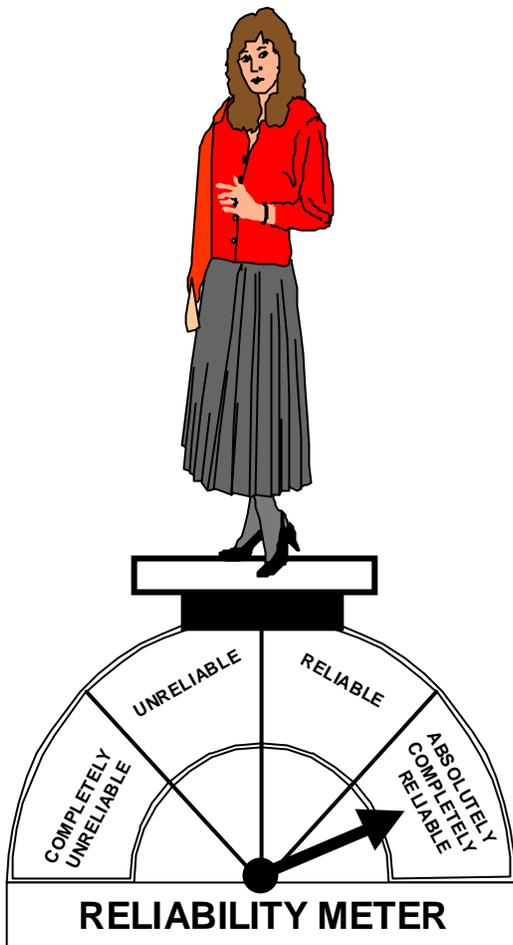
FSO RESPONSIBILITIES

While the basic responsibility for protecting classified information rests with the cleared employee, the FSO has the task of educating that employee, keeping PCL related records, and submitting timely reports on changes affecting PCLs.



There is much the FSO can do to speed up the PCL process to save time for both the FSO and the government. The most obvious way to shorten the PCL process is *not to use the process unless it is absolutely necessary*. Does the employee really need a clearance, or is the request based on status-seeking, over-enthusiastic contingency planning, as a pre-employment screening tool, or some other such consideration? Reducing the number of clearances is a major goal within the NISP, and IS Reps will be scrutinizing this area during every visit.

This goal of clearance reduction and the avoidance of unnecessary clearances have been incorporated into the NISPOM itself and should be included in your SPP. The SPP should outline your facility's system for limiting personnel security clearances. The essential elements of this system are identification for those who are required to make decisions on a person's *need* for a clearance and those who review that decision. These elements are set within the framework of maintaining the minimum number of clearances necessary to meet contractual obligations. The appropriateness of the numbers and levels of PCLs at your facility will be assessed during reviews and other visits to your facility by the Field Office, based on the needs established by your classified contract.



By submitting a clearance application on behalf of an employee, you are essentially saying that certain prerequisites have been met. DSS depends on you, the FSO, to ascertain the citizenship of the applicant through the viewing of proper documentation; if the applicant is a representative of a foreign interest; if the applicant has had a prior clearance; to provide adverse information if known; and so forth.

The NISPOM Chapter 2, Section 2 provides guidance related to Personnel Security Clearance.

FSO RESPONSIBILITIES AFTER THE PCL HAS BEEN GRANTED

Your responsibility to the employee does not end with the submission of the clearance application papers. The granting of a clearance is only part of the equation. The other part is security education. Immediately this means an "initial briefing," a summary of which may be found in paragraph **3-106** of the NISPOM. Following the initial security briefing, a **newly cleared employee** must read, understand, and sign the SF 312 (Classified Information Non-Disclosure Agreement) **prior to having access to classified information**. Employees that held a previous PCL that was converted or reinstated in accordance with NISPOM paragraphs 2-215 and 2-217 need not sign an additional SF 312, if a record exists showing that they have already signed one. The briefings associated with the security education of cleared employees are discussed in Lesson 8.

DENIAL



Zebediah Smythe applied for a clearance, but was denied due to issues uncovered in the clearance process.

SUSPENSION/ REVOCATION



Denise “Fingers” Malone was caught pocketing a piece of classified hardware. Her SECRET clearance was immediately suspended and subsequently revoked.

ADMINISTRATIVE TERMINATION



Duncan Undersides no longer works on any classified projects. While he continues to work at EWS, his clearance is not necessary so Harriet administratively terminated Duncan’s clearance.

DENIAL

Four official actions lead to an employee *not* holding a Personnel Security Clearance. One is the *denial* of the PCL based on the initial application. In this case, the applicant is deemed unworthy of the clearance based on unfavorable information and the clearance is not issued.

SUSPENSION AND REVOCATION

The other three actions involve an existing clearance. With a *suspension* or *revocation*, as with a denial, the employee is found to be ineligible for the clearance. This finding may be based on a periodic reinvestigation, an adverse information report resulting in a reinvestigation, a report of compromise traced back to an individual, or some other cause. Suspension may end in restoration of access or in revocation of the clearance. The person is usually reinvestigated before the clearance is revoked.

CLEARANCE TERMINATION

Denial, suspension, and revocation are all entirely government determinations. The remaining action, the *clearance termination*, is determined primarily by the contractor. This action does not reflect on the worthiness of the employee. Rather, it is based on the lack of continued need for the clearance. Through clearance terminations, the government is able to cut back on the huge number of cleared personnel, thus eliminating the time and money spent on periodic reinvestigations and files maintenance for unneeded clearances. In a clearance termination, the employee (1) terminates from your company, or (2) continues to work at your company, either on another project or perhaps on unclassified parts of the same project. The chart on page 5-29 gives a brief run-down of the procedures on the part of the contractor (FSO) for terminating clearances.

SUMMARY

A Personnel Security Clearance (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 PCL being granted. A National Agency Check with Local Agency Check and Credit Check (NACLIC) is the basic investigative requirement for a SECRET or CONFIDENTIAL clearance. A Single Scope Background Investigation (SSBI) is required for a TOP SECRET clearance. When findings are acceptable, DISCO issues a Letter of Consent to notify the facility that a personnel clearance has been granted. Although being granted a PCL is not a right, an applicant for a PCL is entitled to the provisions of due process if a clearance is denied. The determination to deny a PCL is made by DOHA. Once granted, a PCL remains subject to revocation by DOHA. When a PCL is no longer required, it must be terminated. FSOs must ensure that clearance applications are submitted only when necessary, that they are accurate and complete, that PCL records are properly maintained, and cleared employees are educated in their security responsibilities.

How to Avoid Delays

- Request only essential clearances.
- Use the Electronic Personnel Security Questionnaire (EPSQ).
If you cannot use electronic version, contact your IS Rep.
- Ensure, as far as possible, through a careful review that all forms are completed fully and correctly.
- Be sure to address all mailings correctly.
- Prepare and submit packets promptly .

4 - REVIEW EXERCISES

Complete the following exercises for review and practice. *Multiple-choice questions may have one or more correct choices.*



1. A Personnel Security Clearance (PCL) is an a_____
d_____ that an individual is eligible, from a security point of view,
for a_____ to c_____
i_____ of the same or lower category as the level of PCL being
granted.
2. In its processing of an individual for a PCL, DISCO either makes a favorable
determination and grants the PCL or refers the case to DOHA for a final determination.

 True False
3. Only DOHA is authorized to deny or revoke a PCL.

 True False
4. Both DISCO and DOHA are components of the Defense Security Service.

 True False
5. The official notification that a PCL has been granted is called a L_____ of
C_____.

- b. _____
- c. _____
- d. _____

8. Match the descriptions with the PCL actions. Descriptions may apply to more than one action.

PCL Actions		Descriptions
_____	Denial	a. usually entails a reinvestigation of the cleared person.
_____	Suspension	b. determination made primarily by the contractor.
_____	Revocation	c. determination made entirely by the government.
_____	Clearance Termination	d. action taken when a cleared person no longer requires a clearance. e. due process is followed. f. based on issues related to initial application for clearance. g. individual is deemed ineligible for the clearance.

4 - SOLUTIONS & REFERENCES



1. Administrative determination, access, classified information. (p. 4-2).
2. True. (p. 4-3).
3. True. (p. 4-3).
4. False. (p. 4-3).
5. Letter of Consent. (p. 4-3).
6. Your description should include the following points: Honesty, good judgment, reliability, and trustworthiness. (p. 4-8).
7. See the four ways listed on (p. 4-10 & 4-13)
8. c, e, f, g Denial.

c, g Suspension.

a, c, e, g Revocation.

b, d Clearance termination.

(pp. 4-6, 12).

**USE THE
DEFENSE**

HOTLINE

**TO REPORT FRAUD, WASTE,
& SECURITY VIOLATIONS
RELATING TO
DOD CONTRACTS.**

800/424-9098-toll free

hotline@dodig.osd.mil or www.dodig.osd.mil/hotline



**OR WRITE:
DEFENSE HOTLINE
THE PENTAGON
WASHINGTON, D.C.
20301-1900**

**IDENTITIES OF WRITERS & CALLERS
FULLY PROTECTED.**